Attorney's Docket No.: [redacted]50-009952-US(PAR) [redacted] *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Express Mail No.: EL627421175US
In re application of: Juha SALOKANNEL **Group No.:**
Serial No.: 0 /
Filed: Herewith **Examiner:**
For: METHOD FOR TRANSMITTING AN ENCRYPTION NUMBER IN A COMMUNICATION SYSTEM AND A COMMUNICATION SYSTEM

Commissioner of Patents and Trademarks
Washington, D.C. 20231

#3/Prov't Papers
9/28/01

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country : Finland
Application Number : 19992769
Filing Date : 22 December 1999

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 CFR 1.4(f) (emphasis added.)

SIGNATURE OF ATTORNEY

Reg. No.: 24,622

Clarence A. Green

Type or print name of attorney

Tel. No.: (203) 259-1800

Perman & Green, LLP

P.O. Address

425 Post Road, Fairfield, CT 06430

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 23.10.2000

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Corporation** **Espoo**
Patenttihakemus nro Patent application no	**19992769**
Tekemispäivä Filing date	**22.12.1999**
Kansainvälinen luokka International class	**H04Q**

Keksinnön nimitys
Title of invention

"Menetelmä salausluvun välittämiseksi tiedonsiirtojärjestelmässä ja tiedonsiirtojärjestelmä"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

41

Menetelmä salausluvun välittämiseksi tiedonsiirtojärjestelmässä ja tiedonsiirtojärjestelmä

Nyt esillä oleva keksintö kohdistuu oheisen patenttivaatimuksen 1 johdanto-osan mukaiseen menetelmään salausluvun välittämiseksi tiedonsiirtojärjestelmässä. Keksintö kohdistuu lisäksi oheisen patenttivaatimuksen 9 johdanto-osan mukaiseen tiedonsiirtojärjestelmään.

Kehitteillä on erilaisia langattomia tiedonsiirtojärjestelmiä, joilla langattomia toimistoympäristöön tarkoitettuja tiedonsiirtojärjestelmiä, ns. lähiverkkoja (LAN, Local Area Network), on pyritty toteuttamaan. Useat langattomat tiedonsiirtojärjestelmät perustuvat radiosignaalien käyttöön tiedonsiirrossa. Eräs tällainen kehitettävänä oleva radiotiedonsiirtoon perustuva tiedonsiirtojärjestelmä lähiverkkoa varten on ns. HIPERLAN (HIgh PErformance Radio Local Area Network). Tällaisesta radioverkosta käytetään myös nimitystä laajakaistainen radioverkko (BRAN, Broadband Radio Access Network).

Kehitteillä olevassa HIPERLAN-tiedonsiirtojärjestelmän versiossa 2 tavoitteena on päästä jopa yli 30 Mbit/s tiedonsiirtonopeuteen maksimiyhteysvälin ollessa muutamia kymmeniä metrejä. Tällainen järjestelmä soveltuu käytettäväksi samassa rakennuksessa esim. yhden toimiston sisäisenä lähiverkkona. Kehitteillä on myös ns. HIPERACCESS-tiedonsiirtojärjestelmä, jossa pyritään samaan tiedonsiirtonopeuteen kuin mainitussa HIPERLAN/2-tiedonsiirtojärjestelmässä, mutta yhteysväli pyritään saamaan muutamiin satoihin metreihin, jolloin HIPERACCESS-järjestelmä soveltuu käytettäväksi alueellisena lähiverkkona esimerkiksi oppilaitoksissa ja suuremmissa rakennuskomplekseissa.

Esimerkkinä käytettävän HIPERLAN/2-järjestelmän siirtoyhteyskerroksessa DLC käytettävä MAC-kehysrakenne (Medium Access Control) on pelkistetysti esitettynä oheisessa kuvassa 1b. Tietokehys FR koostuu ohjauskentistä C, kuten RACH (Random Access Channel), BCCH (Broadcast Control CHannel), ja FCCH (Frame Control CHannel) sekä tietokentästä D, joka käsittää määrätyn määrän aikajaksoja TS1, TS2, ..., TSn (time slots), joissa varsinaista hyötyinformaatiota voidaan lähettää.

Kukin ohjauskenttä C sekä tietokentän aikajaksoissa välitettävät paketit sisältävät edullisesti virheentarkistustietoa, jotka tietokehyksen lähettävä yhteysasema AP1 on laskenut ja lisännyt tietokehyksen ohjauskenttiin C sekä aikajaksoissa TS1, TS2, ..., TSn lähetettäviin paketteihin. Tämä tarkistustieto on sopivimmin ao. kentän sisältämän informaation perusteella laskettu tarkistussumma, kuten CRC (Cyclic Redundancy Check). Vastaanottavassa langattomassa päätelaitteessa MT1 virheentarkistusinformaation avulla voidaan tutkia, onko tiedonsiirrossa mahdollisesti ollut virheitä. Kentässä C, D voi olla myös useampia tällaisia tarkistustietoja, jotka on laskettu osasta kentän sisältämää informaatiota. Esim. HIPERLAN/2-järjestelmässä FCCH-ohjauskenttä koostuu pienemmistä informaatioelementeistä, joille kullekin lasketaan tarkistustieto. Näiden informaatioelementtien määrä kussakin tietokehyksessä voi vaihdella. Kaikissa tietokehyksissä ei välttämättä ole FCCH-ohjauskenttää, jolloin myös informaatioelementtien määrä on nolla.

Tiedonsiirto HIPERLAN/2-järjestelmässä perustuu aikajakoiseen multipleksointiin TDMA (Time Division Multiple Access), jolloin samalla kanavalla voi olla useampia samanaikaisia yhteyksiä, mutta kullekin yhteydelle on mainitusta kehyksestä varattu oma aikajakso, jossa tietoa lähetetään. Koska kaikissa samanaikaisissa yhteyksissä ei tiedonsiirtomäärä ole yleensä vakio, vaan vaihtelee ajallisesti, käytetään ns. sopeutuvaa TDMA-menetelmää, jossa kullekin tiedonsiirtoyhteydelle varattavien aikajaksojen lukumäärä voi vaihdella nollasta maksimiin riippuen kulloisestakin kuormitustilanteesta sekä yhteydelle varatusta tiedonsiirtokapasiteetista.

Aikajakoisen multipleksoinnin toimimiseksi on samaan solmuun yhteydessä olevien päätelaitteiden oltava synkronoituja toisiinsa ja solmun lähetykseen. Tämä on aikaansaatavissa esim, siten, että langattoman päätelaitteen vastaanotin vastaanottaa signaaleja jollakin kanavalla. Mikäli kanavalla ei havaita signaalia, vastaanotin siirtyy vastaanottamaan toiselle kanavalle, kunnes kaikki kanavat on tutkittu tai on löydetty sellainen kanava, jossa on havaittu signaalia, joka on jonkin yhteysaseman lähettämää. Tätä signaalia vastaanottamalla ja demoduloimalla voidaan selvittää kyseisen yhteysaseman ohjauskanavan BCCH lähetyshetki ja synkronoida päätelaite tämän perusteella. Joissakin tapauksissa päätelaite voi havaita useamman kuin yhden yhteysaseman

signaalia, jolloin päätelaite valitsee edullisesti sen yhteysaseman, jonka signaalinvoimakkuus vastaanottimessa on suurin ja suorittaa synkronoinnin tähän yhteysasemaan.

Sen jälkeen kun päätelaite on synkronoitu yhteysasemaan, voi päätelaite aloittaa yhteydenmuodostuksen tähän yhteysasemaan kytkeytymiseksi. Se voidaan suorittaa edullisesti siten, että päätelaite lähettää RACH-ohjauskanavassa yhteydenmuodostuspyynnön yhteysasemalle. Käytännössä tämä tarkoittaa sitä, että päätelaite lähettää RACH-ohjauskanavalle varatussa aikajaksossa ja yhteysasema samanaikaisesti kuuntelee kanavan liikennettä, eli vastaanottaa signaaleja käyttämällään kanavataajuudella. Havaittuaan, että jokin päätelaite lähettää yhteydenmuodostuspyyntösanoman, suorittaa yhteysasema yhteydenmuodostuksessa tarvittavat toimenpiteet, kuten resurssien varaamisen yhteydelle, mikäli mahdollista. Resurssien varaamisessa huomioidaan yhteydelle pyydetty palvelun laatutaso, joka vaikuttaa mm. yhteydelle varattavien aikajaksojen lukumäärään. Yhteysasema informoi päätelaitetta siitä, onko yhteyden muodostus mahdollinen vai ei. Mikäli yhteys on saatu muodostettua, lähettää yhteysasema BCCH-ohjauskentässä tiedot mm. yhteydelle varatuista lähetysaikajaksoista, vastaanottoaikajaksoista, yhteyden tunnisteesta, salausta varten salausluvun, jne. Lähetys- ja vastaanottoaikajaksojen lukumäärä ei välttämättä ole sama, koska useissa tapauksissa siirrettävän informaation määrä ei ole sama molempiin suuntiin. Esim. Internet-selainta käytettäessä lähetetään päätelaitteesta huomattavasti vähemmän informaatiota kuin päätelaitteeseen vastaanotetaan informaatiota. Tällöin päätelaitteen kannalta lähetysaikajaksoja tarvitaan vähemmän kuin vastaanottoaikajaksoja. Lisäksi yhteydelle varattujen aikajaksojen lukumäärä voi edullisesti vaihdella eri kehyksissä kulloisenkin informaation siirtotarpeen mukaan. Yhteysaseman ohjaimeen on muodostettu ns. jaksottaja (scheduler), jonka eräänä tehtävänä on edellä mainittu aikajaksojen varaaminen eri yhteyksiä varten. Jaksottaja on toteutettu edullisesti sovellusohjelmana yhteysaseman ohjaimessa.

Koska lähiverkoissa tarvitaan kaksisuuntaista tiedonsiirtoa, myös radiotiellä tarvitaan kaksisuuntaista tiedonsiirtoyhteyttä. Aikajakoisessa järjestelmässä tämä voidaan toteuttaa joko siten, että kehyksen aikajaksoista osa varataan lähetykseen langattomalta päätelaitteelta yhteys-

asemalle (uplink) ja osa varataan yhteysasemalta langattomaan päätelaitteeseen (downlink), tai siten, että kumpaakin tiedonsiirtosuuntaa varten varataan oma taajuuskaistansa. HIPERLAN/2-järjestelmässä on esitetty ensin mainitun menetelmän käyttöönottoa, jolloin yhteysasema ja siihen yhteydessä olevat langattomat päätelaitteet eivät lähetä samanaikaisesti.

Tiedonsiirtoyhteyttä muodostettaessa langaton päätelaite kuuntelee, minkä yhteysasemien signaaleja on vastaanotettavissa. Langaton päätelaite mittaa edullisesti vielä signaalien voimakkuuksia ja valitsee esim. sen yhteysaseman, jonka signaali sillä hetkellä on voimakkain. Tämän jälkeen langaton päätelaite ja yhteysasema suorittavat yhteydenmuodostussignalointia mm. yhteydessä käytettävien parametrien, kuten tarvittavan tiedonsiirtonopeuden, yhteystyypin, tiedonsiirtokanavan, aikajaksojen sekä yhteystunnuksen välittämiseksi.

Langaton päätelaite tyypillisesti mittaa myös yhteyden aikana yhteydessä käytettävän yhteysaseman signaalin voimakkuutta sekä muiden mahdollisten kuuluvuusalueella olevien yhteysasemien signaalien voimakkuuksia. Mikäli jollakin muulla yhteysasemalla havaitaan riittävässä määrin voimakkaampi signaalinvoimakkuus kuin sillä hetkellä käytettävän yhteysaseman signaalinvoimakkuus, voidaan suorittaa yhteydensiirto tälle toiselle yhteysasemalle (handover), kuten on tunnettua.

Hiperlan/2-tiedonsiirtojärjestelmä käsittää yhteysaseman AP (Access Point), yhteysaseman ohjaimen APC (Access Point Controller) ja langattomia päätelaitteita MT (Mobile Terminal). Lisäksi Hiperlan/2-järjestelmä voidaan järjestää tiedonsiirtoyhteyteen muihin tiedonsiirtojärjestelmiin, kuten langalliseen ja langattomaan televerkkoon, Internet-verkkoon jne. Tiedonsiirto yhteysaseman ja langattoman päätelaitteen välillä suoritetaan langattomasti radioteitse. Tällöin salakuuntelumahdollisuuksien pienentämiseksi voidaan suorittaa salaus, jossa radiotiellä välitettäväksi tarkoitettu informaatio ensin salataan ja sen jälkeen lähetetään. Salausta varten on Hiperlan/2-tiedonsiirtojärjestelmään ehdotettu muodostettavaksi salausavainjoukkoa. Tämän salausavainjoukon avaimia käytetään ennalta määrätyssä järjestyksessä kulloinkin lähetettävän tietokehyksen sisältämän informaation salaamiseksi. Salausavaimen pituus on esim. 56 bittiä. Tämän salausavaimen ja tietyn sa-

lausalgoritmin avulla muodostetaan salattu informaatio. Salausalgoritmi ja salausavainjoukko ovat tallennettuina yhteysasemaan sekä langattomiin päätelaitteisiin. Tällöin salausalgoritmia ja salausavaimia ei tarvitse lähettää radiotien yli, mikä pienentää salausmenetelmän paljastumisen ja väärinkäytön mahdollisuutta.

Salausavaimen ja -algoritmin paljastumisen vaikeuttamiseksi ei jatkuvasti käytetä samaa salausavainta, vaan salausavainta vaihdetaan määrävälein. Tämän vuoksi Hiperlan/2-järjestelmään on ehdotettu sellaista ratkaisua, jossa yhteysasemalta lähetetään langattomaan päätelaitteeseen ns. salausluku (salausavaimen tahdistussiemen, seed), jonka perusteella langaton päätelaite voi muodostaa salauksessa käyttämänsä salausavaimen. Salausluku (ja salausavain) on aina kehyskohtainen, eli se vaihtuu Hiperlan/2-järjestelmässä kahden millisekunnin välein. Kuitenkaan tätä salauslukua ei tarvitse välittää langattomaan päätelaitteeseen jokaista kehystä varten erikseen, vaan järjestely on toteutettu siten, että langaton päätelaite tietää salausavainsekvenssin ja voi yhden vastaanottamansa salausluvun perusteella selvittää myös seuraavien kehysten salauksessa käytettävän salausavaimen. Tämä kuitenkin edellyttää sitä, että langaton päätelaite pysyy synkronoituneena yhteysaseman lähetykseen. Mikäli jostakin syystä langaton päätelaite ei havaitse kaikkia kehyksiä, tai langaton päätelaite ei jostain muusta syystä enää ole synkronoituna yhteysaseman lähetykseen, ei langattomalla päätelaitteella ole oikeaa tietoa salausavaimesta. Myös tilanteessa, jossa langaton päätelaite on suorittanut yhteysaseman vaihdon (hand over), ei langattomalla päätelaitteella ole tietoa tämän uuden yhteysaseman kulloinkin käyttämästä salausavaimesta. Tämän vuoksi on esitetty, että salausluvun lähetys suoritetaan määrävälein, jolloin langaton päätelaite pystyy suorittamaan jälleen salauksen/salauksen purkamisen sen jälkeen, kun langaton päätelaite on vastaanottanut uuden salausluvun.

Salauslukujen lähetysväli vaikuttaa mm. siihen, kuinka nopeasti esimerkiksi yhteysaseman vaihtotilanteessa langaton päätelaite pystyy lähettämään salattua informaatiota. Tällöin, mitä nopeammin salauslukuja lähetetään, sitä nopeammin yhteysaseman vaihdon jälkeen langaton päätelaite pystyy lähettämään ja vastaanottamaan salattua informaatiota. Tämä salauslukujen pieni lähetysväli aiheuttaa kuitenkin sen epä-

kohdan, että tiedonsiirtojärjestelmää kuormitetaan suhteellisen paljon näillä salauslukujen lähettämisillä.

Nyt esillä olevan keksinnön eräänä tarkoituksena on aikaansaada menetelmä ja tiedonsiirtojärjestelmä, jossa salauslukujen lähetysväliä voidaan pidentää ja silti saavuttaa mahdollisimman nopea toipuminen esimerkiksi yhteysaseman vaihtotilanteessa ja synkronoitumisen kadotessa. Keksintö perustuu siihen ajatukseen, että yhteysasema lähettää salausluvun langattomalle päätelaitteelle yhteysaseman vaihdon yhteydessä. Nyt esillä olevan keksinnön mukaiselle menetelmälle on tunnusomaista se, mitä on esitetty oheisen patenttivaatimuksen 1 tunnusmerkkiosassa. Nyt esillä olevan keksinnön mukaiselle tiedonsiirtojärjestelmälle on tunnusomaista se, mitä on esitetty oheisen patenttivaatimuksen 9 tunnusmerkkiosassa.

Nyt esillä olevalla keksinnöllä saavutetaan merkittäviä etuja tunnetun tekniikan mukaisiin ratkaisuihin verrattuna. Keksinnön mukaista menetelmää käyttäen voidaan salauslukujen lähetysväliä harventaa ja silti salaukseen synkronoituminen langattomassa päätelaitteessa voidaan suorittaa nopeasti yhteyaseman vaihtotilanteessa. Koska salauslukujen lähetysväliä voidaan harventaa, myös tiedonsiirtojärjestelmän kuormitus pienenee vastaavasti, kuten myös yhteysasemassa ja langattomassa päätelaitteessa tarvittava prosessointi. Lisäksi langattomien päätelaitteiden kokonaistehonkulutusta saadaan pienennettyä, koska langaton päätelaite ei tarpeettomasti siirry lepotilasta normaaliin toimintatilaan vastaanottamaan tietokehyksiä, joissa jollekin toiselle langattomalle päätelaitteelle lähetetään salausluku. Nopea salaukseen synkronoituminen merkitsee myös sitä, että yhteysaseman vaihtotilanteessa yhteyden katkeamisilta voidaan paremmin välttyä kuin tunnetun tekniikan mukaisissa tiedonsiirtojärjestelmissä.

Nyt esillä olevaa keksintöä selostetaan seuraavassa tarkemmin viitaten samalla oheisiin piirustuksiin, joissa

kuva 1a esittää keksinnön erään edullisen suoritusmuodon mukaista tiedonsiirtojärjestelmää pelkistettynä lohkokaaviona,

kuva 1b esittää erästä tietokehystä HIPERLAN/2-järjestelmässä,

kuva 2 esittää keksinnön erään edullisen suoritusmuodon mukaista langatonta päätelaitetta pelkistettynä lohkokaaviona,

kuva 3 esittää keksinnön erään edullisen suoritusmuodon mukaista yhteysasemaa ja yhteysaseman ohjainta pelkistettynä lohkokaaviona,

kuva 4 esittää pelkistetysti keksinnön erään edullisen suoritusmuodon mukaisen menetelmän toteutusta tietokehysmuodossa,

kuva 5 esittää pelkistetysti keksinnön erään edullisen suoritusmuodon mukaisen menetelmän yhteydessä toteutettua salausta pelkistettynä kaaviona, ja

kuva 6 esittää keksinnön erään edullisen suoritusmuodon mukaisessa tiedonsiirtojärjestelmässä sovellettavia protokollapinoja pelkistetysti.

Seuraavassa keksinnön edullisen suoritusmuodon mukaisen tiedonsiirtojärjestelmän 1 kuvauksessa käytetään esimerkkinä kuvan 1a mukaista HIPERLAN/2-järjestelmää, mutta on selvää, että keksintöä ei ole rajoitettu ainoastaan tähän järjestelmään. Tiedonsiirtojärjestelmä 1 koostuu langattomista päätelaitteista MT1—MT4, yhdestä tai useammasta yhteysasemasta AP1, AP2 (Access Point) sekä yhteysaseman ohjaimesta APC1, APC2 (Access Point Controller). Yhteysaseman AP1, AP2 ja langattoman päätelaitteen MT1—MT4 välille muodostetaan radioyhteys, jossa siirretään mm. yhteyden muodostamisessa tarvittavia signaaleita ja yhteyden aikana informaatiota, kuten Internet-sovelluksen tietopaketteja. Yhteysaseman ohjain APC1, APC2 kontrolloi yhteysaseman AP1, AP2 toimintaa ja niiden kautta muodostettuja yhteyksiä langattomiin päätelaitteisiin MT1—MT4. Yhteysaseman ohjaimessa APC1, APC2 on kontrolleri 19 (kuva 3), jonka sovellusohjelmistoon yhteysaseman toimintoja on toteutettu, kuten yhteysaseman jaksottaja (Scheduler), joka suorittaa erilaisia ajoitustoimenpiteitä sinänsä tunnetusti. Tällaisessa radioverkossa voi useita yhteysaseman ohjaimia APC1, APC2 olla tiedonsiirtoyhteydessä toisiinsa sekä muihin tietoverkkoihin, kuten Internet-tietoverkkoon, UMTS-matkaviestinverkkoon

(Universal Mobile Terminal System) jne., jolloin langaton päätelaite MT1—MT4 voi kommunikoida esim. Internet-tietoverkkoon kytketyn päätelaitteen TE1 kanssa. On selvää, että keksintöä voidaan soveltaa myös sellaisissa tiedonsiirtojärjestelmissä, joissa ei ole yhteysaseman ohjainta APC1, APC2, vaan vastaavat toiminnot on toteutettu yhteysasemassa AP1, AP2.

Kuvassa 2 on esitetty pelkistettynä lohkokaaviona keksinnön erään edullisen suoritusmuodon mukainen langaton päätelaite MT1. Langaton päätelaite MT1 käsittää edullisesti tietojenkäsittelytoimintoja PC sekä tiedonsiirtovälineet COM tiedonsiirtoyhteyden muodostamiseksi langattomaan lähiverkkoon. Langaton päätelaite voi olla muodostettu myös siten, että tietojenkäsittelylaitteeseen, kuten kannettavaan tietokoneeseen, on liitetty esim. lisäkortti, joka käsittää mainitut tiedonsiirtovälineet COM. Tietojenkäsittelytoiminnot PC käsittävät edullisesti suorittimen 2, kuten mikroprosessorin, mikrokontrollerin tai vastaavan, näppäimistön 3, näyttöelimen 4, muistivälineet 5, ja liitäntävälineet 6. Lisäksi tietojenkäsittelytoiminnot PC voivat käsittää audiovälineet 7, kuten kaiuttimen 7a, mikrofonin 7b, ja koodekin 7c, jolloin käyttäjä voi käyttää langatonta päätelaitetta MT1 myös mm. puheen siirtämiseen. Langattomasta päätelaitteesta MT1 lähiverkkoon lähetettäväksi tarkoitettu informaatio siirretään edullisesti liitäntävälineiden 6 kautta tiedonsiirtovälineisiin COM. Vastaavasti lähiverkosta 1 langattomassa päätelaitteessa MT1 vastaanotettu informaatio siirretään tietojenkäsittelytoimintoihin PC mainittujen liitäntävälineiden 6 kautta.

Tiedonsiirtovälineet COM käsittävät mm. antennin 30, suurtaajuusosan 8, kooderin 20, dekooderin 21, salauslohkon 9, salauksen purkulohkon 10, ohjauselimen 11 sekä referenssioskillaattorin 12. Suurtaajuusosa 8 käsittää edullisesti mm. suodattimia, modulaattorin ja demodulaattorin (ei esitetty). Lisäksi tiedonsiirtovälineissä COM on muistia 13 mm. tiedonsiirrossa tarvittavien lähetys- ja vastaanottopuskureiden muodostamiseksi sekä salausavaintaulukon ja salaussekvenssin tallentamiseksi. Kooderissa 20 suoritetaan tietokehyksien sisältämän informaation koodaus. Koodattu informaatio johdetaan suurtaajuusosaan 8 moduloitavaksi ja johdettavaksi radiotaajuisena signaalina lähetys tiedonsiirtokanavaan CH (kuva 1a). Vastaavasti dekooderissa palautetaan tiedonsiirtokanavasta vastaanotettu ja demodulaattorissa demoduloitu

koodattu informaatio edullisesti tietokehysmuotoon. Referenssioskillaattorilla 12 muodostetaan tarvittavat ajoitukset lähetyksen ja vastaanoton synkronoimiseksi yhteysaseman lähetykseen ja vastaanottoon. Referenssioskillaattoria 12 voidaan käyttää myös ohjauselimen 11 ajoitussignaalien muodostamiseen. On selvää, että referenssioskillaattorin 12 muodostamaa taajuutta ei sellaisenaan voida käyttää kanavataajuuden asettamisessa ja ohjauselimen 11 ajoitussignaalien muodostamisessa, jolloin käytännön sovelluksissa käytetään taajuuden muunnosvälineitä (ei esitetty) referenssioskillaattorin 12 taajuuden muuntamiseksi radio-osassa tarvittaviksi taajuuksiksi ja ohjauselimen 11 toiminnan ohjaukseen soveltuvaksi taajuudeksi.

Yhteysasemassa AP1 (kuva 3) on vastaavasti ensimmäiset tiedonsiirtovälineet 15, 23—26 tiedonsiirtoyhteyden muodostamiseksi langattomiin päätelaitteisiin MT1—MT4. Keksinnön mukainen langaton lähiverkko 1 voidaan toteuttaa myös paikallisena lähiverkkona, josta ei ole yhteyttä ulkoisiin tietoverkkoihin. Tällöin saattaa riittää yksi yhteysasema AP1, johon lähiverkon langattomat päätelaitteet MT1—MT4 ovat yhteydessä. Langattomassa lähiverkossa yhdestä tai useammasta yhteysasemasta AP1, AP2 on edullisesti järjestetty tiedonsiirtoyhteys 16 tietojenkäsittelylaitteeseen S, jota yleisesti kutsutaan palvelintietokoneeksi tai lyhyemmin palvelimeksi. Tällaisessa palvelimessa on sinänsä tunnetusti keskitettynä yrityksen tietokantoja, sovellusohjelmia, jne. Käyttäjät voivat tällöin käynnistää langattoman päätelaitteen MT1 kautta palvelimelle S asennettuja sovelluksia. Palvelin S tai yhteysasema AP1 voi lisäksi käsittää toiset tiedonsiirtovälineet 17 tiedonsiirtoyhteyden muodostamiseksi johonkin muuhun tietoverkkoon, kuten Internet-tietoverkkoon tai UMTS-matkaviestinverkkoon.

Yhteysaseman AP1, AP2 tiedonsiirtovälineet käsittävät yhden tai useamman oskillaattorin 22 toiminnassa tarvittavien taajuuksien muodostamiseksi, salauslohkon 23, salauksen purkulohkon 25, kooderin 24, dekooderin 26 sekä suurtaajuusosan 15, mikä on sinänsä tunnettua.

Kullekin yhteysasemalle AP1, AP2 ja langattomalle päätelaitteelle MT1—MT4 on määritetty yksilöivä tunnus, jolloin yhteysasema AP1, AP2 on selvillä siitä, mitä langattomia päätelaitteita MT1—MT4 kulloinkin on kytkeytyneenä yhteysasemaan AP1, AP2. Vastaavasti tunnuksi-

en perusteella langattomat päätelaitteet MT1—MT4 erottavat eri yhteysasemien AP1, AP2 lähettämät kehykset toisistaan. Näitä tunnuksia voidaan käyttää myös sellaisessa tilanteessa, jossa langattoman päätelaitteen MT1—MT4 yhteys siirtyy yhdestä yhteysasemasta AP1 toiseen yhteysasemaan AP2, esim. yhteyden laadun heikentymisen seurauksena.

Tiedonsiirtoa varten on langaton päätelaite MT1 kytkettävä tiedonsiirtoyhteyteen lähiverkkoon 1. Tämä voidaan suorittaa edullisesti siten, että langattomassa päätelaitteessa MT1 käynnistetään verkko-ohjain, tai vastaava sovellusohjelma, johon on muodostettu ohjelmakoodit lähiverkkoon 1 kytkeytymiseksi sekä tietojen siirtämiseksi langattoman päätelaitteen MT1 ja lähiverkon 1 välillä. Verkko-ohjaimen käynnistämisen yhteydessä suoritetaan tarvittavat toimenpiteet mm. langattoman päätelaitteen tiedonsiirtovälineiden COM toimintaparametrien asettamiseksi. Tällöin tiedonsiirtovälineiden COM vastaanotin aloittaa signaalien vastaanoton jollakin lähiverkon kanavataajuudella. Mikäli signaalia ei tietyn ajan kuluessa havaita, vaihdetaan kuunneltavaa kanavaa. Siinä vaiheessa kun jollakin kuunneltavalla kanavataajuudella on havaittu signaalia, tiedonsiirtovälineiden COM vastaanottimen vastaanottama signaali demoduloidaan ja johdetaan dekoodattavaksi, jolloin voidaan selvittää radiosignaalissa lähetetty informaatio, kuten on tunnettua. Tästä dekoodatusta signaalista, joka sopivimmin on tallennettu vastaanottopuskuriin tiedonsiirtovälineiden muistiin 13, etsitään tietokehyksen BCCH-ohjauskentän tunniste. Tämä BCCH-ohjauskentän tunniste on tietyssä kohdassa tietokehystä, joten sen jälkeen kun tunniste on löydetty, on BCCH-ohjauskentän sijainti vastaanottopuskurissa selvillä. BCCH-ohjauskenttä sisältää mm. tietokehyksen lähettäneen yhteysaseman tunnisteen (AP ID), lähiverkon tunnisteen (NET ID), tietokehyksen numeron, salausluvun, tarvittaessa alustusvektorin, sekä tietoa FCCH-ohjauskentän pituudesta, modulointitavasta ja koodauksesta.

Langaton päätelaite MT1 synkronoituu tämän yhteysaseman AP1 lähetykseen. Langaton päätelaite MT1 pyytää yhteyden muodostusta lähettämällä yhteysasemalle AP1 RACH-sanoman sille varatulla ajanhetkellä. Esimerkiksi kuvan 1b mukaisessa kehysrakenteessa RACH-sanoma voidaan lähettää lähetys- ja vastaanottoaikajaksojen jälkeen, ennen seuraavaa BCCH-ohjauskenttää. Sanomassa langaton päätelaite MT1

lähettää tietoa mm. yhteydelle haluttavasta palvelun laatutasosta ja yhteystyypistä, kuten multimediayhteys, datayhteys, puheyhteys. Yhteyden tyyppi ja palvelun laatutaso vaikuttavat mm. yhteydelle varattavien aikajaksojen TS1—TSn lukumäärään.

Yhteysaseman ohjain APC1 tutkii sanoman ja selvittää esim. resurssien varaustaulukosta tai vastaavasta, kuinka paljon yhteysasemalla AP1 on sillä hetkellä resursseja vapaana. Mikäli resursseja on riittävästi pyydettyä palvelun laatutasoa vastaavan yhteyden muodostamiseksi, yhteysaseman ohjain APC1 varaa yhteydelle tarvittavat resurssit. Yhteydelle muodostetaan yhteysaseman ohjaimen APC1 muistivälineisiin 14 lähetys- ja vastaanottojonot (-puskurit), joita käytetään vastaanotettujen pakettien väliaikaiseen tallennukseen ja lähetystä odottavien pakettien väliaikaiseen tallennukseen. Lisäksi kullekin yhteydelle annetaan yhteystunnus, jolloin varmistetaan tiedon siirtyminen oikeaan kohteeseen. Yhteydelle voidaan valita myös prioriteetti, jolloin kulloinkin vapaana olevia resursseja, kuten lähetys- ja vastaanottoaikajaksoja, annetaan prioriteettijärjestyksessä. Riippuen mm. resurssitarpeesta voidaan eri yhteyksille varata tietokehyksen FR tietokentästä eri määrä aikajaksoja TS1—TSn. Myös lähetykseen ja vastaanottoon varattujen aikajaksojen lukumäärä voi olla erilainen samallakin yhteydellä, kuten jo aikaisemmin tässä selityksessä on mainittu. Yhteyksille varattujen aikajaksojen TS1—TSn määrä voi vielä vaihdella kehyskohtaisesti, jolloin kussakin tietokehyksessä FR yhteydelle varattujen aikajaksojen TS1—TSn lukumäärä voi vaihdella nollasta maksimiin. Tietokehyksen sisältämien lähetys- ja vastaanottoaikajaksojen sijainti tietokehyksessä välitetään edullisesti FCCH-ohjauskentässä.

Sen jälkeen kun yhteys lähiverkkoon 1 on saatu muodostettua, voidaan aloittaa tietojen siirto palvelimen S ja langattoman päätelaitteen MT1 välillä edullisesti jollakin protokollalla, kuten IP (Internet Protocol). Kuvassa 6 on esitetty tätä tiedonsiirtoa protokollapinojen avulla. Protokollapinoista on esitetty sovelluskerros AL (Application Layer), verkkokerros CL+NL (Convergence Layer + Network Layer), siirtoyhteyskerros DL (Data Link Layer) sekä fyysinen kerros PHY (Physical Layer). Radiotiellä, eli yhteysaseman AP1 ja langattoman päätelaitteen MT1 välillä protokollapinon siirtoyhteyskerros käsittää tässä edullisessa suoritusmuodossa alimpana MAC-kerroksen (Media Access Control), joka

huolehtii radiotien käyttämisestä langattoman päätelaitteen MT1 ja yhteysaseman AP1 välisessä liikennöinnissä, kuten salauksesta, kanavien varauksesta pakettien lähetyksessä ja vastaanotossa. Tässä selityksessä kuvataan lähinnä MAC-kerroksen tietokehyksiä FR. On selvää, että myös muiden protokollakerrosten yhteydessä voidaan suorittaa salaustoimenpiteitä, mutta sillä ei tämän keksinnön kannalta ole merkitystä sinänsä, joten niitä ei tässä yhteydessä käsitellä tarkemmin.

Yhteysaseman ohjaimeen APC1, APC2 muodostettu jaksottaja 18 suorittaa mm. yhteysaseman AP1, AP2 tietokehysten FR ajoituksen ja lähetys- ja vastaanottoaikajaksojen varaamisen aktiivisena olevien yhteyksien lähetystä odottaville paketeille. Jaksottaja kytkee yhteysaseman vastaanottimen vastaanottamaan radiosignaalia kehyksen RACH-kentälle varatuksi ajaksi. Tällöin langattomat päätelaitteet MT1—MT4 voivat suorittaa edellä esitetyn yhteyden muodostuspyynnön välittämisen lisäksi erilaisen mittaustiedon välitystä yhteysasemalle.

Selostetaan seuraavaksi keksinnön erään edullisen suoritusmuodon mukaisen menetelmän toimintaa. Siinä vaiheessa kun langaton päätelaite MT1 on kytkeytynyt ensimmäiseen yhteysasemaan AP1 ja vastaanottanut salausluvun KI, on langaton päätelaite MT1 asettanut salaussekvenssilaskurin SC (kuva 2) salauslukua vastaavaan arvoon. Jos salausluku on indeksi salausavaintaulukkoon ST, josta eräs edullinen esimerkki on kuvassa 5, voidaan salaussekvenssilaskurin SC arvoksi asettaa suoraan tämä salausluku. Tämän jälkeen langaton päätelaite MT1 tarkkailee yhteysaseman AP1 lähetystä ja aina kehyksen vaihdon yhteydessä muuttaa salaussekvenssilaskurin arvoa siten, että se osoittaa edullisesti seuraavaan salausavaimeen salausavaintaulukossa ST. Kehyksen vaihtuminen on havaittavissa siitä, että yhteysasema AP1 lähettää (seuraavan) BCCH-ohjauskentän. Tämän BCCH-ohjauskentän vastaanoton yhteydessä langaton päätelaite MT1 voi tarvittaessa suorittaa myös paikallisen kellon tahdistuksen sen pitämiseksi synkronoituneena yhteysasemaan AP1. Salaustaulukon ST viimeisen salausavaimen jälkeen salaussekvenssilaskuri SC asetetaan osoittamaan sopivimmin salaustaulukon ST alkuun.

Yhteysasema AP1 lähettää tiettyjen MAC-kehysten BCCH-kentässä tietoa kaikille kyseiseen yhteysasemaan AP1 yhteydessä oleville lan-

gattomille päätelaitteille (Broadcast Frame) tai osalle niistä (Subbroadcast Frame). Tällöin kukin näistä langattomista päätelaitteista vastaanottaa ainakin BCCH-ohjauskentässä lähetetyn informaation ja selvittää sen perusteella, milloin ao. langattomalle päätelaitteelle lähetetään informaatiota ja milloin se itse voi lähettää informaatiota. Tämän jälkeen voi langaton päätelaite mahdollisesti siirtyä tehon säästämiseksi lepotilaan (sleep mode), jolloin lepotila asetetaan päättyväksi joko ennen seuraavan useammille langattomille päätelaitteille tarkoitetun yleisen BCCH-ohjauskentän lähetystä, tai ennen kyseiselle langattomalle päätelaitteelle MT1 varattua lähetys- tai vastaanottoaikajaksoa. Lepotilassa langattoman päätelaitteen MT1 radio-osa on asetettu tehonsäästötilaan tai kytketty pois päältä. Salaussekvenssilaskuri SC voidaan kuitenkin päivittää, koska langaton päätelaite MT1 on selvillä siitä, kuinka monen MAC-kehyksen ajan se on lepotilassa.

Salausta keksinnön erään edullisen suoritusmuodon mukaisessa tiedonsiirtojärjestelmässä on esitetty oheisessa kuvassa 5 pelkistettynä kaaviona. Salausluku KI ja tarvittaessa myös alustusvektori IV on lähetetty ainakin kerran langattomalle päätelaitteelle MT1. Alustusvektorilla on satunnaisseksenssigeneraattorille RS asetettu tietty alkuarvo. Vastaavasti langattomassa päätelaitteessa MT1 on suoritettu langattoman päätelaitteen satunnaissekvenssigeneraattorin alkuarvon asetus. Siinä vaiheessa kun yhteysasemalla AP1 on lähetettävänä langattomalle päätelaitteelle informaatiota, muodostetaan kyseisellä hetkellä käytössä olevan salausavaimen perusteella salaussekvenssi satunnaissekvenssigeneraattorissa RS. Tämä salaussekvenssi johdetaan yhdistelylohkoon XOR, jossa suoritetaan salaussekvenssin ja lähetettävän informaation välillä edullisesti ehdoton tai -operaatio (XOR, Exclusive Or) biteittäin salatun informaation muodostamiseksi. Yhdistelylohkosta XOR salattu informaatio johdetaan lähetettäväksi edullisesti yhdessä tai useammassa tietokentässä D.

Langattoman päätelaitteen MT1 tiedonsiirtovälineillä COM suoritetaan tiedonsiirtokanavasta vastaanotetun ja demodulaattorissa demoduloidun, salatussa muodossa olevan informaation salauksen purku edullisesti seuraavasti. Langattomassa päätelaitteessa MT1 lasketaan salausavaimen, satunnaissekvenssigeneraattorin ja alustusvektorin perusteella salaussekvenssi vastaavasti kuin yhteysasemalla AP1. Salattu

informaatio ja salaussekvenssi johdetaan erottelulohkoon XOR', josta ulostulona saadaan lähetetty informaatio salaamattomassa muodossa.

On selvää, että nyt esillä olevan keksinnön yhteydessä voidaan käyttää myös muita menetelmiä informaation salaamiseksi salausavaimen avulla, kuin edellä on esitetty.

Tilanteessa, jossa langaton päätelaite MT1 vaihtaa yhteyden jollekin toiselle yhteysasemalle AP2 tai ensimmäinen yhteysasema AP1 suorittaa pakotetun yhteysaseman vaihdon, langaton päätelaite MT1 suorittaa yhteysaseman vaihdon yhteydessä normaalin yhteysaseman vaihtosignaloinnin tämän toisen yhteysaseman AP2 kanssa. Tätä on kuvattu kehyksenä, joka on merkitty viitteellä HO oheisessa kuvassa 4. Tässä vaiheessa langaton päätelaite MT1 ei kuitenkaan voi enää käyttää muistissaan olevaa salauslukua, koska langaton päätelaite MT1 ei tiedä, mitä salauslukua tällä toisella yhteysasemalla AP2 käytetään sillä hetkellä. Toinen yhteysasema AP2 suorittaa väliajoin salausluvun lähetyksiä, mutta sen lisäksi nyt esillä olevan keksinnön mukaisessa menetelmässä yhteysasema AP2 lähettää salausavaimen yhteysaseman vaihdon jälkeen, koska seuraavaan salausluvun lähetykseen kuluva aika voi olla jopa niin pitkä, että yhteys voisi jopa katketa.

Salausavaimen lähetys voidaan toteuttaa edullisesti seuraavasti (kuva 4). Vastaanotettuaan tiedon salausluvun lähetystarpeesta, toinen yhteysasema AP2 valitsee seuraavan sopivan hetken salausavaimen lähettämiselle. Yhteysasema AP2 valitsee sopivimmin seuraavan sellaisen BCCH-ohjauskentän, jota ei käytetä aikaisemmin tässä selityksessä mainittuna yleisenä BCCH-ohjauskenttänä, joita kuvaan 4 on esimerkinomaisesti merkitty viitteellä BC. Tällä järjestelyllä ei tarpeettomasti aiheuteta vastaanottotoimenpiteitä ja ei lisätä tehonkulutusta tarpeettomasti muissa langattomissa päätelaitteissa. Yhteysasema AP2 lähettää salausluvun ainakin yhden kerran, mutta varmistaakseen sen, että langaton päätelaite MT1 saa salausluvun oikein vastaanotettua, voi yhteysasema lähettää sen useammankin kerran, esim. kolme kertaa peräkkäin. Tämä toisto voi olla tarpeen mm. sellaisissa tilanteissa, joissa langaton päätelaite MT1 on solun reunalla, tai muussa sellaisessa kohdassa, jossa signaalinvoimakkuus on vaimentunut. Kuvaan 4 on merkitty viitteellä YS näitä yhteydenvaihdon jälkeen lähetettäviä yhtä

tai useampaa salausluvun lähetystä ja vastaavasti viitteellä NS normaalia, väliajoin suoritettavaa salausluvun lähetystä.

Yhteydenvaihdosta voidaan ilmoittaa yhteysasemalle AP1, AP2 useilla eri tavoilla. Esimerkiksi yhteen yhteysasemaan AP1 yhteydessä oleva langaton päätelaite MT1 voi itse lähettää yhteydenvaihtopyynnön jollekin toiselle yhteysasemalle AP2. Langaton päätelaite MT1 voi tässä yhteydessä ilmoittaa yhteydenvaihdosta sille yhteysasemalle AP1, johon se sillä hetkellä on yhteydessä ja josta yhteys siirretään toiselle yhteysasemalle AP2. Tällöin, jos yhteysasemien AP1 AP2 välille on järjestetty tiedonsiirtoyhteys, voi tämä ensimmäinen yhteysasema AP1 ilmoittaa toiselle yhteysasemalle AP2, että salauslukuja on tarve lähettää useammin. Eräänä toisena vaihtoehtona on se, että yhteysasema AP1, johon langaton päätelaite MT1 sillä hetkellä on yhteydessä, pakottaa langattoman päätelaitteen MT1 suorittamaan yhteydenvaihdon. Myös tässä tilanteessa tämä ensimmäinen yhteysasema AP1 voi ilmoittaa toiselle yhteysasemalle AP2, että salauslukuja on tarve lähettää useammin.

Keksinnön mukaisen menetelmän toiminnot voidaan yhteysasemassa AP1, AP2 toteuttaa edullisesti yhteysaseman ohjaimen kontrollerin 19 sovellusohjelmistossa.

Keksintöä voidaan soveltaa myös muissa kuin tässä esimerkissä käytetyssä HIPERLAN/2-järjestelmässä. Esimerkiksi GSM-järjestelmän mukaisessa matkaviestinjärjestelmässä (ei esitetty) yhteysasemaa AP1, AP2 vastaa tukiasema ja yhteysasemaohjainta APC1, APC2 vastaa tukiasemaohjain, joka tukiasemien välityksellä on radiotiedonsiirtoyhteydessä langattomiin viestimiin.

Vastaavasti WCDMA-järjestelmässä (ei esitetty) yhteysasemaa AP1, AP2 vastaa tukiasema (Node-B) ja yhteysasemaohjainta APC1, APC2 vastaa radioverkko-ohjain (Radio Network Controller).

Myös muut kuin aikajakoiset (TDMA, Time Division Multiple Access) järjestelmät voivat tulla kyseeseen, esim. koodijakoinen järjestelmä (CDMA, Code Division Multiple Access), tai taajuusjakoinen järjestelmä (FDMA, Frequency Division Multiple Access), tai näiden eri järjestel-

mien kombinaatio. Tällöin koodijakoisessa järjestelmässä aikajaksoja vastaavana ominaisuutena (lähetysjaksona) on koodijakso, ja taajuusjakoisessa järjestelmässä taajuusjakso.

On selvää, että nyt esillä olevaa keksintöä ei ole rajoitettu ainoastaan edellä esitettyihin suoritusmuotoihin, vaan sitä voidaan muunnella oheisten patenttivaatimusten puitteissa.

Patenttivaatimukset:

1. Menetelmä salausluvun välittämiseksi langattomassa tiedonsiirtojärjestelmässä (1), joka käsittää langattomia päätelaitteita (MT1—MT4), ja ainakin ensimmäisen yhteysaseman (AP1), ja toisen yhteysaseman (AP2), jossa menetelmässä:
- määritetään joukko salausavaimia,
- valitaan kussakin mainitussa yhteysasemassa (AP1, AP2) mainitusta joukosta salausavaimia kulloinkin yksi käytettäväksi mainitun yhteysaseman (AP1, AP2) ja langattoman päätelaitteen (MT1—MT4) välillä välitettävän informaation salaamisessa,
- lähetetään yhteysasemalta (AP1, AP2) väliajoin tietoa kulloinkin valittuna olevasta salausavaimesta,
- muodostetaan tiedonsiirtoyhteys langattoman päätelaitteen (MT1—MT4) ja ensimmäisen yhteysaseman (AP1) välille informaation siirtämiseksi, ja
- suoritetaan yhteydenvaihto, jossa muodostetaan tiedonsiirtoyhteys toisen yhteysaseman (AP2) ja langattoman päätelaitteen (MT1—MT4) välille,

tunnettu siitä, että menetelmässä lähetetään yhteydenvaihdon yhteydessä langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) valittuna olevasta salausavaimesta.

2. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että määritetään kullekin salausavaimelle mainitussa joukossa salausavaimia salausluku (KI), jolloin mainittuna tietona valittuna olevasta salausavaimesta käytetään mainittua salauslukua (KI).

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, jossa informaatiota siirretään tietokehyksissä (FR), **tunnettu** siitä, että salausavainta vaihdetaan jokaisen tietokehyksen (FR) yhteydessä.

4. Patenttivaatimuksen 3 mukainen menetelmä, jossa osaa tietokehyksistä käytetään yleisinä tietokehyksinä informaation lähettämiseksi toiselta yhteysasemalta (AP2) useammalle kuin yhdelle langattomalle päätelaitteelle (MT1—MT4), **tunnettu** siitä, että mainittu tieto salausavaimesta lähetetään jossakin muussa tietokehyksessä kuin mainitussa yleisessä tietokehyksessä.

5. Jonkin patenttivaatimuksen 1—4 mukainen menetelmä, **tunnettu** siitä, että tallennetaan mainittu joukko salausavaimia mainittuihin yhteysasemiin (AP1, AP2) ja langattomaan päätelaitteeseen (MT1—MT4).

6. Jonkin patenttivaatimuksen 1—5 mukainen menetelmä, **tunnettu** siitä, että langaton päätelaite (MT1—MT4) ilmoittaa mainitulle toiselle yhteysasemalle (AP2) yhteydenvaihtotarpeesta, jolloin mainittu toinen yhteysasema (AP2) lähettää langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) sillä hetkellä valittuna olevasta salausavaimesta.

7. Jonkin patenttivaatimuksen 1—5 mukainen menetelmä, **tunnettu** siitä, että langaton päätelaite (MT1—MT4) ilmoittaa mainitulle ensimmäiselle yhteysasemalle (AP1) yhteydenvaihtotarpeesta, että mainittu ensimmäinen yhteysasema (AP1) lähettää mainitulle toiselle yhteysasemalle (AP2) tiedon yhteydenvaihdosta, jolloin mainittu toinen yhteysasema (AP2) lähettää langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) sillä hetkellä valittuna olevasta salausavaimesta.

8. Jonkin patenttivaatimuksen 1—5 mukainen menetelmä, **tunnettu** siitä, että ensimmäinen yhteysasema (AP1) suorittaa pakotetun yhteydenvaihdon, jossa mainittuun ensimmäiseen yhteysasemaan tiedonsiirtoyhteydessä oleva langaton päätelaite (MT1—MT4) siirretään tiedonsiirtoyhteyteen mainittuun toiseen yhteysasemaan (AP2), että mainittu ensimmäinen yhteysasema (AP1) lähettää mainitulle toiselle yhteysasemalle (AP2) tiedon yhteydenvaihdosta, jolloin mainittu toinen yhteysasema (AP2) lähettää langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) sillä hetkellä valittuna olevasta salausavaimesta.

9. Langaton tiedonsiirtojärjestelmä (1), joka käsittää langattomia päätelaitteita (MT1—MT4), ainakin ensimmäisen yhteysaseman (AP1), ja toisen yhteysaseman (AP2), johon tiedonsiirtojärjestelmään (1) on määritetty joukko salausavaimia, joka yhteysasema (AP1, AP2) käsittää välineet mainitusta joukosta salausavaimia kulloinkin yhden valitsemiseksi

käytettäväksi mainitun yhteysaseman (AP1, AP2) ja langattoman päätelaitteen (MT1—MT4) välillä välitettävän informaation salaamisessa, ja välineet tiedon kulloinkin valittuna olevasta salausavaimesta lähettämiseksi väliajoin yhteysasemalta (AP1, AP2), ja joka tiedonsiirtojärjestelmä (1) käsittää lisäksi välineet tiedonsiirtoyhteyden muodostamiseksi langattoman päätelaitteen (MT1—MT4) ja ensimmäisen yhteysaseman (AP1) välille informaation siirtämiseksi, ja välineet yhteydenvaihdon suorittamiseksi ja tiedonsiirtoyhteyden muodostamiseksi toisen yhteysaseman (AP2) ja langattoman päätelaitteen (MT1—MT4) välille, **tunnettu** siitä, että langaton tiedonsiirtojärjestelmä (1) käsittää lisäksi välineet tiedon toisessa yhteysasemassa (AP2) valittuna olevasta salausavaimesta lähettämiseksi langattomalle päätelaitteelle (MT1—MT4) yhteydenvaihdon yhteydessä.

10. Patenttivaatimuksen 9 mukainen langaton tiedonsiirtojärjestelmä (1), **tunnettu** siitä, että se käsittää lisäksi välineet salausluvun määrittämiseksi kullekin salausavaimelle mainitussa joukossa salausavaimia (ST), jolloin mainittuna tietona valittuna olevasta salausavaimesta on järjestetty käytettäväksi mainittua salauslukua (KI).

11. Patenttivaatimuksen 9 tai 10 mukainen langaton tiedonsiirtojärjestelmä (1), joka käsittää välineet informaation siirtämiseksi tietokehyksissä (FR), **tunnettu** siitä, että salausavainta on järjestetty vaihdettavaksi jokaisen tietokehyksen (FR) yhteydessä.

12. Patenttivaatimuksen 11 mukainen langaton tiedonsiirtojärjestelmä (1), jossa osaa tietokehyksistä on järjestetty käytettäväksi yleisinä tietokehyksinä informaation lähettämiseksi toiselta yhteysasemalta (AP2) useammalle kuin yhdelle langattomalle päätelaitteelle (MT1—MT4), **tunnettu** siitä, että mainittu tieto salausavaimesta on järjestetty lähetettäväksi jossakin muussa tietokehyksessä kuin mainitussa yleisessä tietokehyksessä.

13. Jonkin patenttivaatimuksen 9—12 mukainen langaton tiedonsiirtojärjestelmä (1), **tunnettu** siitä, että mainittu joukko salausavaimia on tallennettu mainittuihin yhteysasemiin (AP1, AP2) ja langattomaan päätelaitteeseen (MT1—MT4).

14. Jonkin patenttivaatimuksen 9—13 mukainen menetelmä, **tunnettu** siitä, että langaton päätelaite (MT1—MT4) käsittää välineet (8, 11, 30) yhteydenvaihtotarpeen ilmoittamisesta mainitulle toiselle yhteysasemalle (AP2), jolloin mainitusta toisesta yhteysasemasta (AP2) on järjestetty lähetettäväksi langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) sillä hetkellä valittuna olevasta salausavaimesta.

15. Jonkin patenttivaatimuksen 9—13 mukainen menetelmä, **tunnettu** siitä, että langaton päätelaite (MT1—MT4) käsittää välineet (8, 11, 30) yhteydenvaihtotarpeen ilmoittamisesta mainitulle ensimmäiselle yhteysasemalle (AP1) yhteydenvaihtotarpeesta, että ensimmäinen yhteysasema (AP1) käsittää välineet tiedon yhteydenvaihdosta lähettämiseksi mainitulle toiselle yhteysasemalle (AP2), jolloin mainitusta toisesta yhteysasemasta (AP2) on järjestetty lähetettäväksi langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) sillä hetkellä valittuna olevasta salausavaimesta.

16. Jonkin patenttivaatimuksen 9—13 mukainen menetelmä, **tunnettu** siitä, että ensimmäinen yhteysasema (AP1) käsittää välineet pakotetun yhteydenvaihdon suorittamiseksi, jossa mainittuun ensimmäiseen yhteysasemaan tiedonsiirtoyhteydessä oleva langaton päätelaite (MT1—MT4) on järjestetty siirrettäväksi tiedonsiirtoyhteyteen mainittuun toiseen yhteysasemaan (AP2), ja välineet tiedon yhteydenvaihdosta lähettämiseksi mainitulle toiselle yhteysasemalle (AP2), jolloin mainitusta toisesta yhteysasemasta (AP2) on järjestetty lähetettäväksi langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) sillä hetkellä valittuna olevasta salausavaimesta.

L3

(57) Tiivistelmä

Keksintö kohdistuu menetelmään salausluvun välittämiseksi langattomassa tiedonsiirtojärjestelmässä (1), joka käsittää langattomia päätelaitteita (MT1—MT4), ja ainakin ensimmäisen yhteysaseman (AP1), ja toisen yhteysaseman (AP2). Menetelmässä määritetään joukko salausavaimia, valitaan kussakin mainitussa yhteysasemassa (AP1, AP2) mainitusta joukosta salausavaimia kulloinkin yksi käytettäväksi mainitun yhteysaseman (AP1, AP2) ja langattoman päätelaitteen (MT1—MT4) välillä välitettävän informaation salaamisessa, lähetetään yhteysasemalta (AP1, AP2) väliajoin tietoa kulloinkin valittuna olevasta salausavaimesta, ja muodostetaan tiedonsiirtoyhteys langattoman päätelaitteen (MT1—MT4) ja ensimmäisen yhteysaseman (AP1) välille informaation siirtämiseksi. Menetelmässä suoritetaan yhteydenvaihto, jossa muodostetaan tiedonsiirtoyhteys toisen yhteysaseman (AP2) ja langattoman päätelaitteen (MT1—MT4) välille. Menetelmässä lisäksi lähetetään yhteydenvaihdon yhteydessä langattomalle päätelaitteelle (MT1—MT4) tietoa toisessa yhteysasemassa (AP2) valittuna olevasta salausavaimesta.

Fig. 4

14

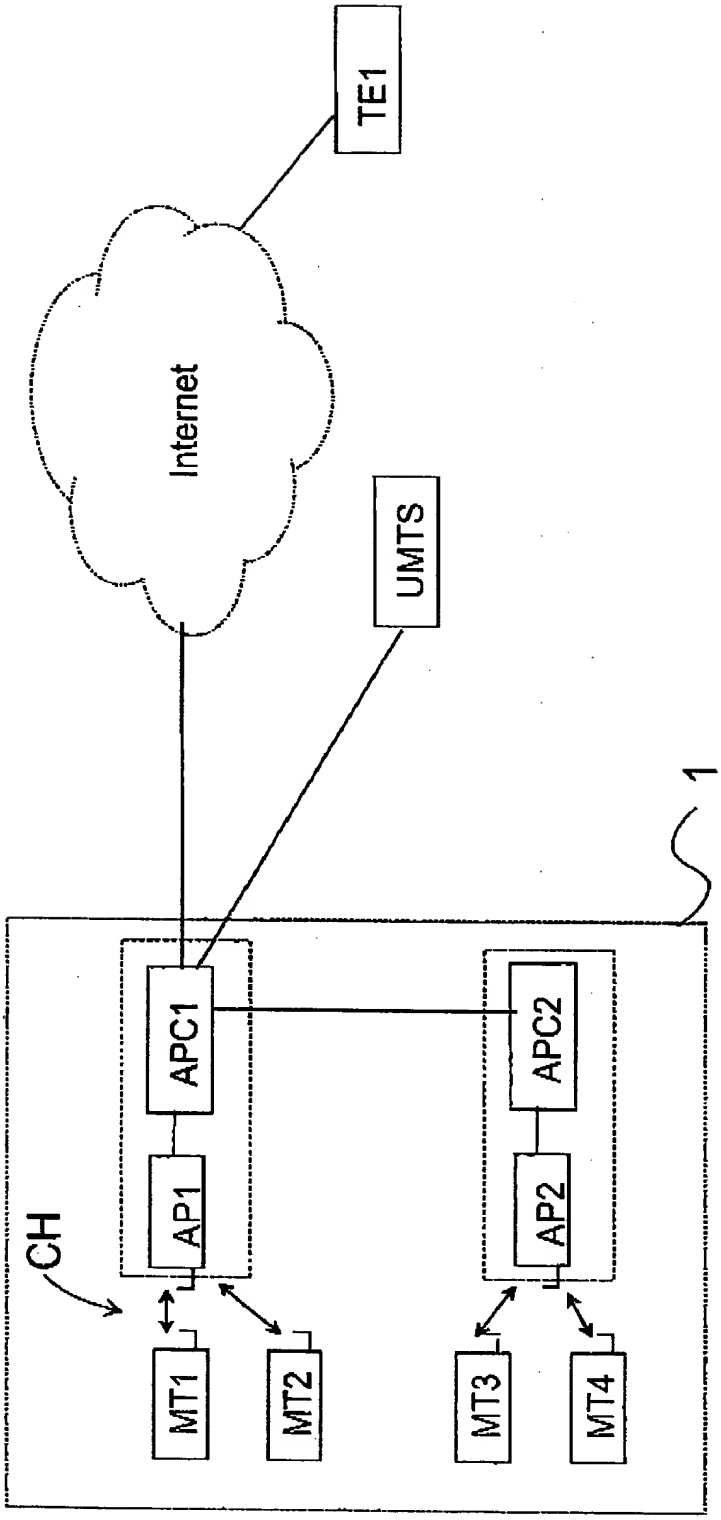

Fig. 1a

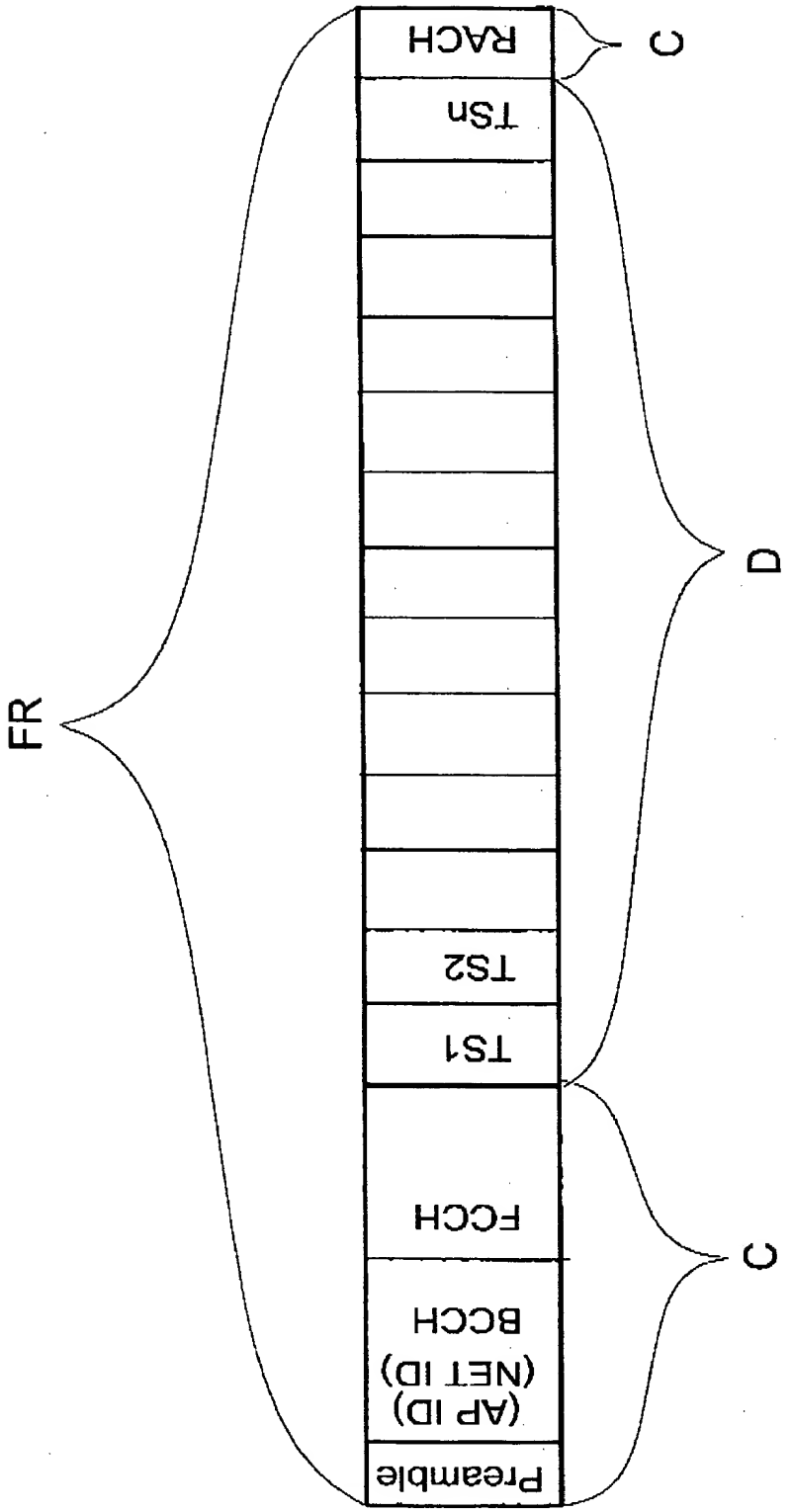

Fig. 1b

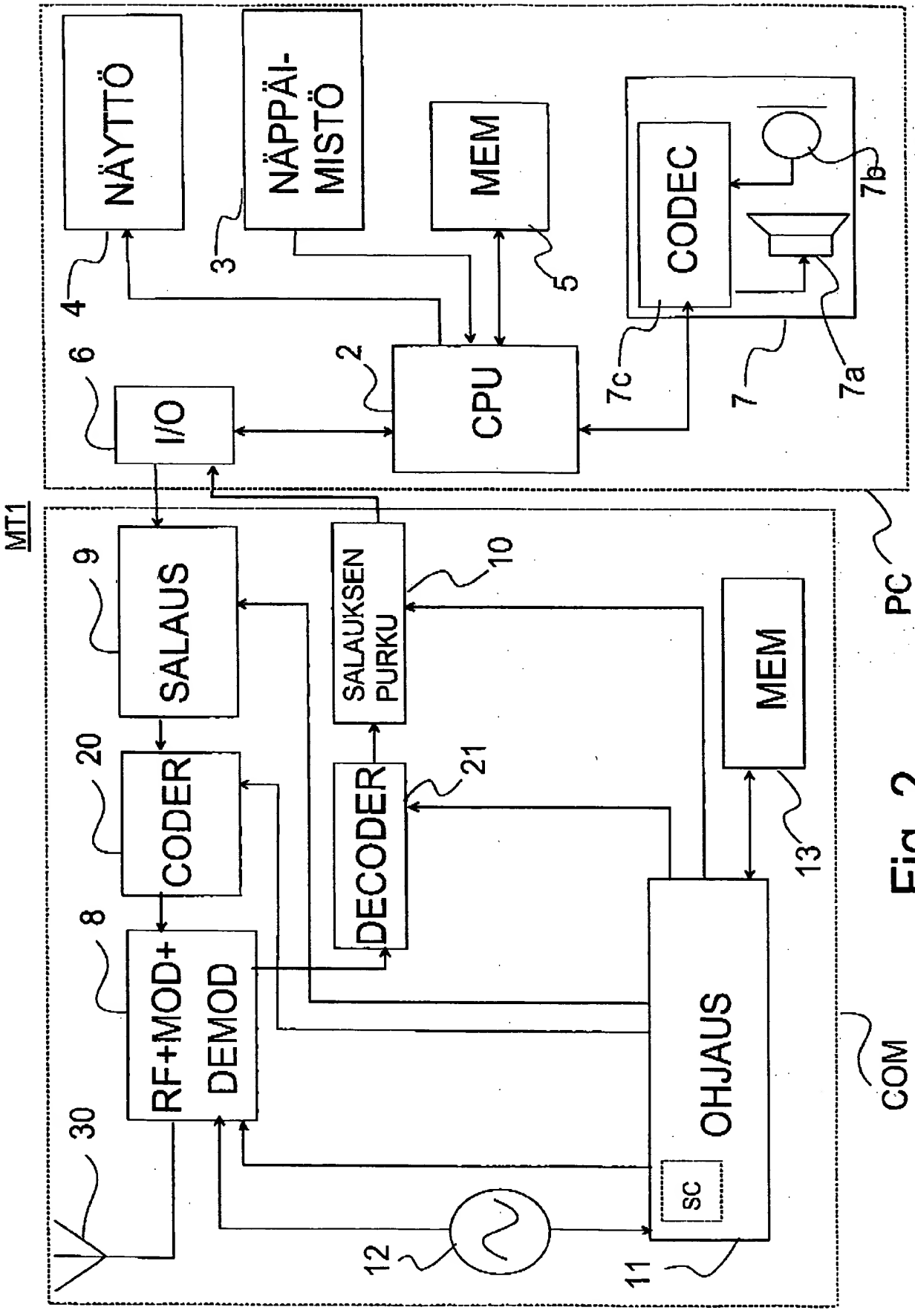
NÄYTTÖ
NÄPPÄI-
MISTÖ
MEM
CODEC
7b
4
3
5
6
2
I/O
CPU
7c
7
7a
PC
MT1
9
SALAUS
SALAUKSEN
PURKU
10
MEM
20
CODER
DECODER
21
13
8
RF+MOD+
DEMOD
OHJAUS
SC
COM
30
12
11

Fig. 2

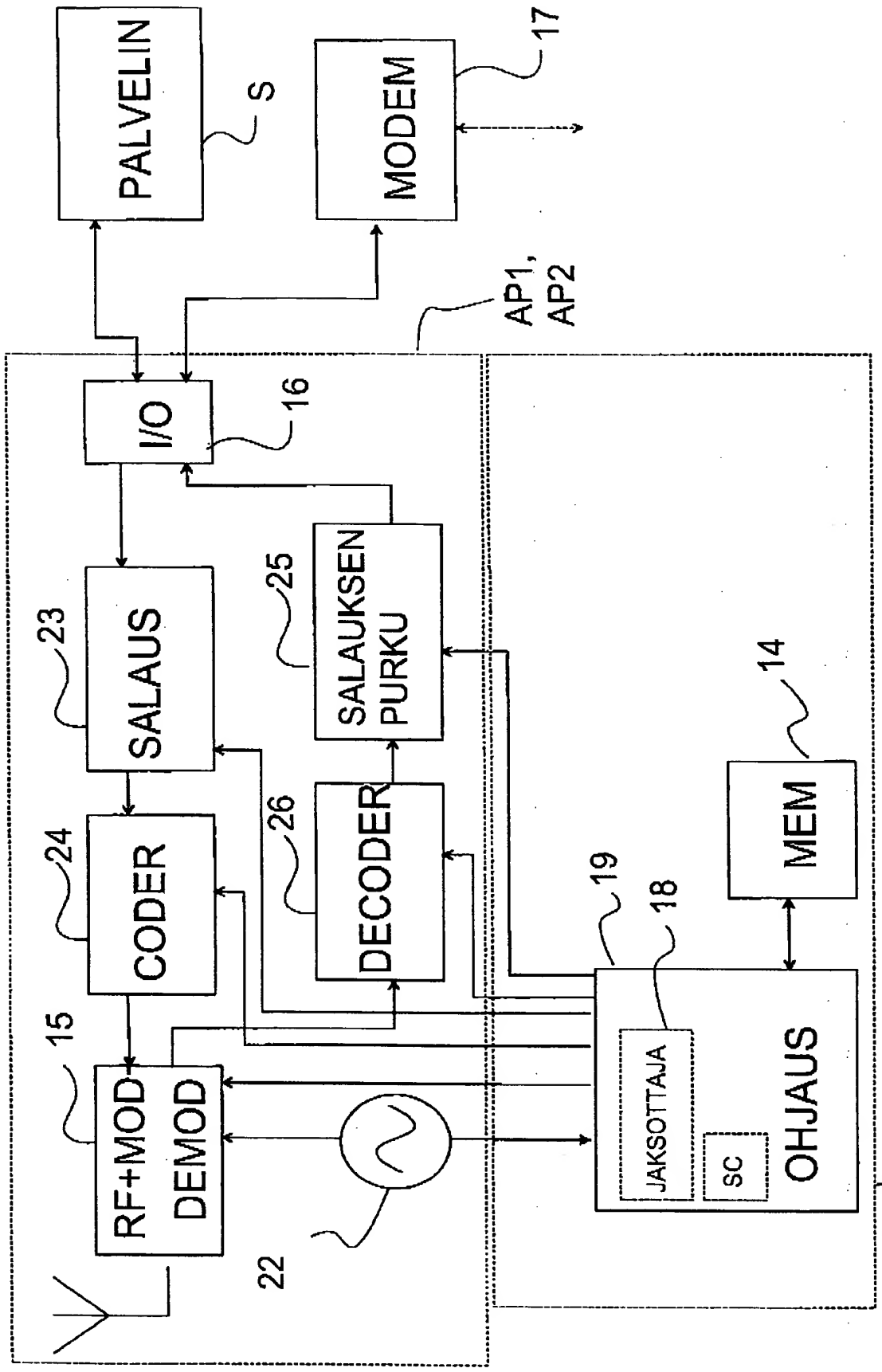
PALVELIN
S
MODEM
17
AP1,
AP2
I/O
16
SALAUS
23
SALAUKSEN
PURKU
25
CODER
24
DECODER
26
MEM
14
19
18
RF+MOD
DEMOD
15
JAKSOTTAJA
SC
OHJAUS
22
APC1, APC2

Fig. 3

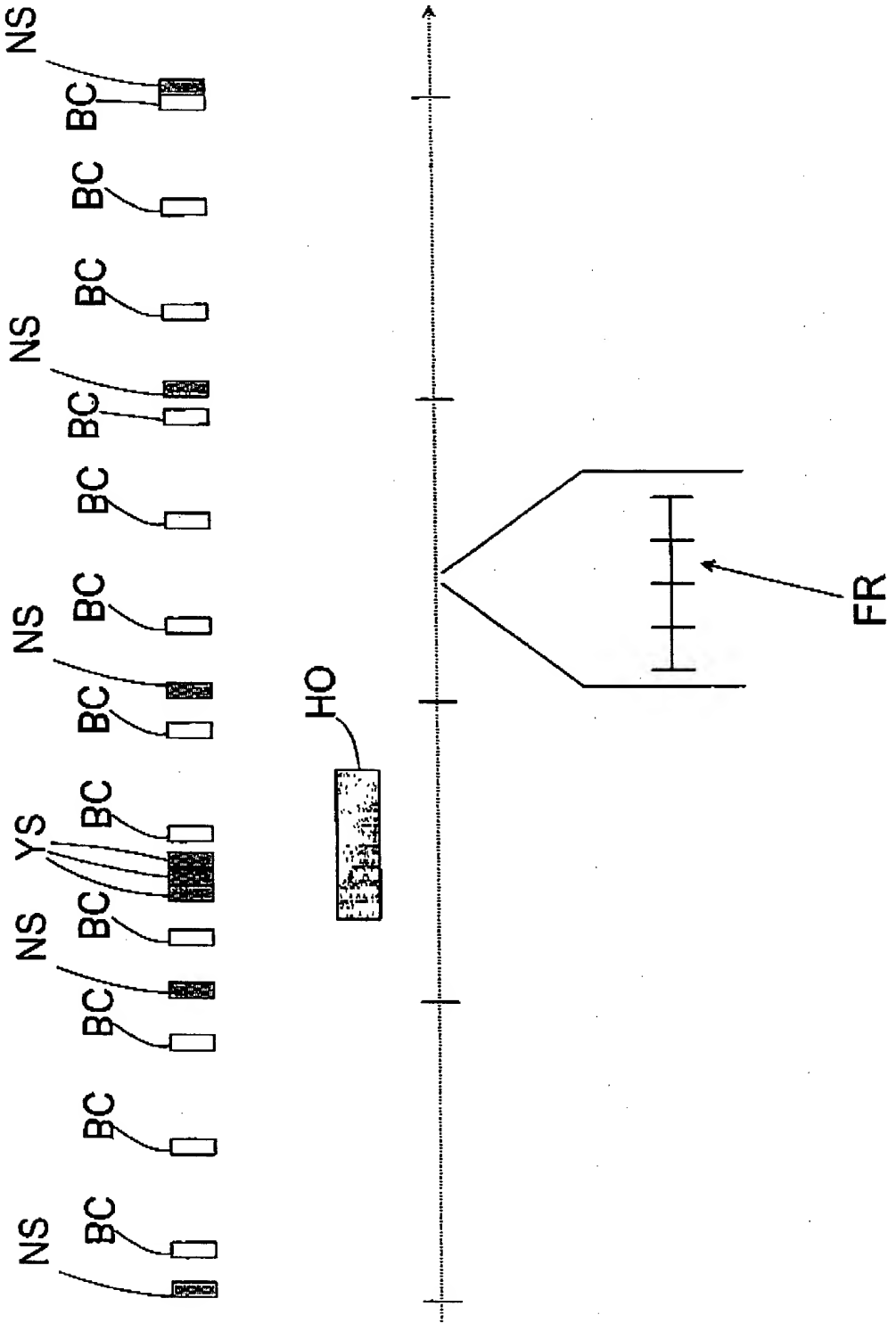

Fig. 4

KI1	Avain 1
KI2	Avain 2
KI3	Avain 3
KI4	Avain 4
KI5	Avain 5
⋮	⋮
KIm-1	Avain M-1
KIm	Avain M

ST

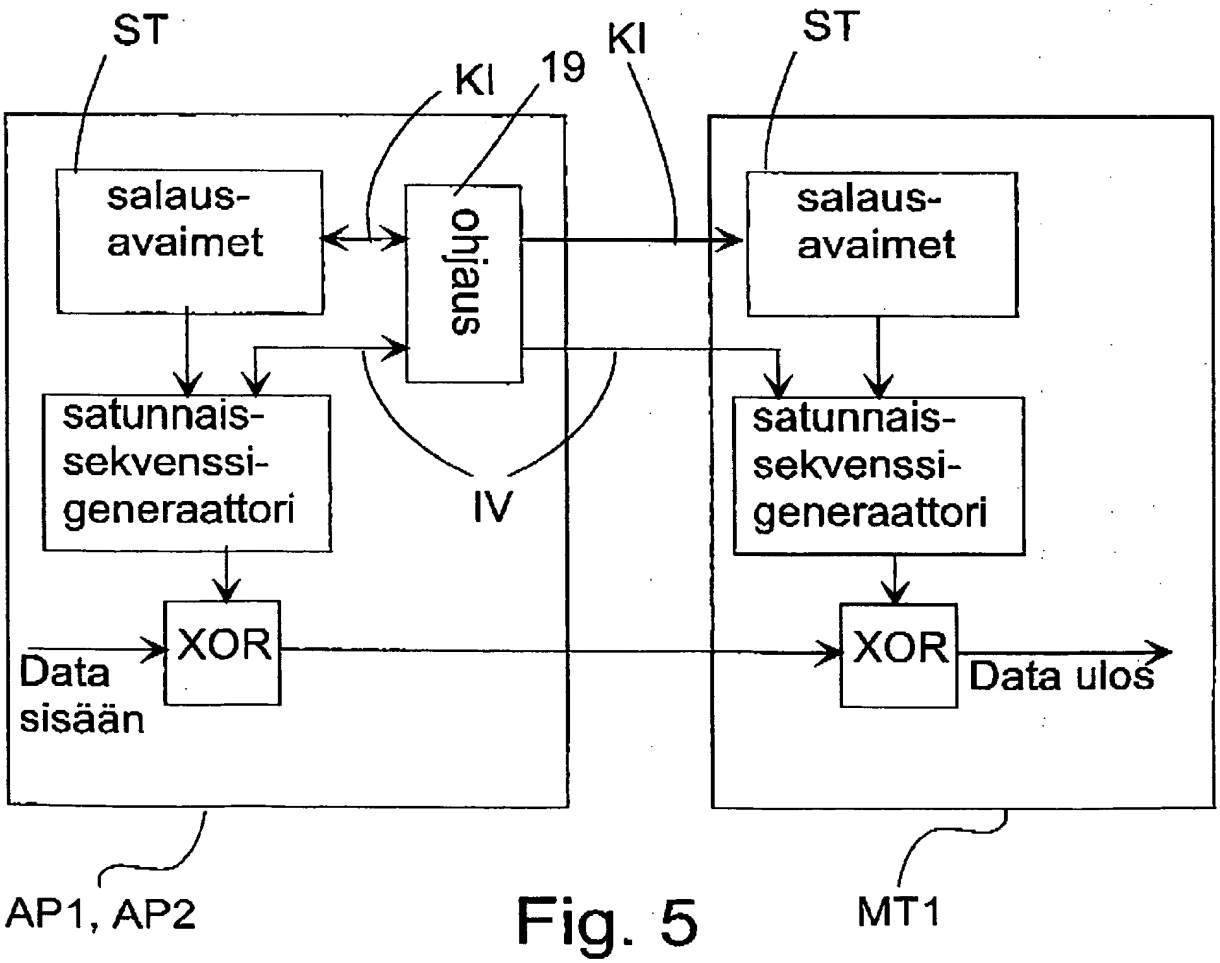

Fig. 5

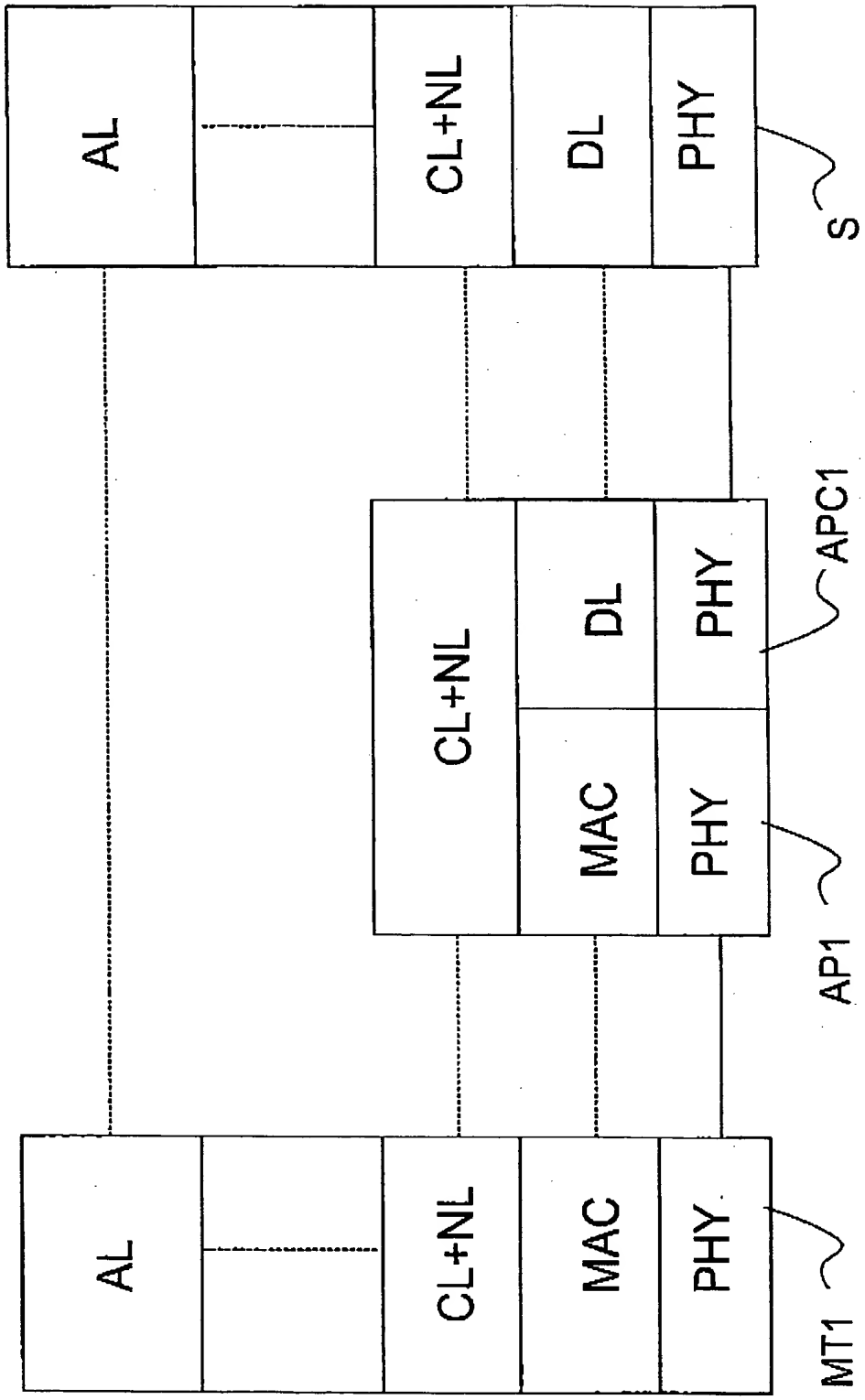

Fig. 6

CERTIFICATE

I, Tuulikki Tulivirta, hereby certify that, to the best of my knowledge and belief, the following is a true translation, for which I accept responsibility, of a certified copy of Finnish Patent Application 19992769 filed on 22 December 1999.

Tampere, 1 November 2000

Tuulikki Tulivirta
Certified Translator (Act 1148/88)

Tampereen Patenttitoimisto Oy
Hermiankatu 6
FIN-33720 TAMPERE
Finland

Method for transmitting an encryption number in a communication system and a communication system

The present invention relates to a method for transmitting an encryption number in a communication system as set forth in the preamble of the appended claim 1. The invention also relates to a communication system as set forth in the preamble of the appended claim 9.

There are various wireless communication systems under development for implementing wireless communication systems for an office environment, so-called local area networks (LAN). Several wireless communication systems are based on the use of radio signals in communication. One such communication system based on radio communication is the so-called HIPERLAN (HIgh PErformance Radio Local Area Network). Such a radio network is also called a broadband radio access network (BRAN).

In version 2 of the HIPERLAN communication system under development, the aim is to achieve a data transmission rate of even more than 30 Mbit/s, the maximum connection distance being some tens of metres. Such a system is suitable for use in the same building *e.g.* as an internal local area network for one office. There is also a so-called HIPERACCESS communication system under development, in which the aim is to achieve the same data transmission rate as in said HIPERLAN/2 communication system, but the aim is to achieve a connection distance of several hundreds of metres, wherein the HIPERACCESS system is suitable for use as a regional local area network for example in schools and larger building complexes.

In the HIPERLAN/2 system which is used as an example, the MAC (Medium Access Control) frame structure used in the data link layer DLC is shown in a reduced manner in the appended Fig. 1b. The data frame FR consists of control fields C, such as RACH (Random Access CHannel), BCCH (Broadcast Control CHannel) and FCCH (Frame Control CHannel), as well as a data field D which comprises a given number of time slots TS1, TS2, ..., TSn, in which it is possible to transmit actual payload information.

Each control field C as well as the packets to be transmitted in the time slots of the data field preferably comprise error checking data which has been calculated by an access point AP1 transmitting the data frame and added into the control fields C of the data frame and to the packets to be transmitted in the time slots TS1, TS2, ..., TSn. This checking data is preferably a checksum calculated on the basis of information contained in said field, such as CRC (Cyclic Redundancy Check). In the receiving mobile terminal MT1, it is possible to use the error checking data to examine if the data transmission possibly contained any errors. There can also be several items of such error checking data in the field C, D, calculated on part of the information contained in the field. For example in the HIPERLAN/2 system, the FCCH control field consists of smaller information elements, for which error checking data is calculated respectively. The number of these information elements may vary in each data frame. All data frames do not necessarily have an FCCH control field, in which case the number of information elements is zero.

Communication in the HIPERLAN/2 system is based on time division multiple access TDMA, wherein there can be several connections simultaneously on the same channel, but in said frame each connection is allotted a time slot of its own, in which data is transmitted. Because the quantity of data to be transmitted is usually not constant in all the simultaneous connections, but it varies in time, a so-called adapted TDMA method is used, in which the number of time slots to be allocated for each data transmission connection may vary from zero to a maximum, depending on the loading situation at each time as well as on the data transmission capacity allocated for the connection.

For the time division multiple access to work, the terminals coupled to the same node must be synchronized with each other and with the transmission of the node. This can be achieved for example in such a way that the receiver of the mobile terminal receives signals on a channel. If no signal is detected on the channel, the receiver shifts to receive on another channel, until all the channels are examined or a channel is found on which a signal is detected that is transmitted from an access point. By receiving and demodulating this signal, it is possible to find out the time of transmission of the control channel BCCH of the access

point in question and to use this to synchronize the terminal. In some cases, the terminal may detect a signal from more than one access points, wherein the terminal preferably selects the access point with the greatest signal strength in the receiver and performs synchronization with this access point.

After the terminal has been synchronized with the access point, the terminal can start a connection set-up to couple to this access point. This can be performed preferably so that the terminal transmits a connection set-up request to the access point on the RACH control channel. In practice, this means that the terminal transmits in a time slot allocated for the RACH control channel and the access point simultaneously listens to communication on the channel, *i.e.* receives signals on the channel frequency used by the same. After detecting that a terminal is transmitting a connection set-up request message, the access point takes the measures required for setting up the connection, such as resource allocation for the connection, if possible. In the resource allocation, the quality of service requested for the connection is taken into account, affecting *e.g.* the number of time slots to be allocated for the connection. The access point informs the terminal if the connection set-up is possible or not. If it has been possible to set up a connection, the access point transmits in the BCCH control field information *e.g.* on the transmission time slots, receiving time slots, connection identifier, *etc.* allocated for the connection. The number of transmission and receiving time slots is not necessarily the same, because in many cases the quantity of information to be transmitted is not the same in both directions. For example, when an Internet browser is used, considerably less information is transmitted from the terminal than information is received at the terminal. Thus, for the terminal, fewer transmission time slots are needed than receiving time slots. Furthermore, the number of time slots allocated for the connection may preferably vary in different frames according to the need to transmit information at the time. The access point controller is provided with a so-called scheduler, which serves *e.g.* the purpose of allocating time slots for different connections as mentioned above. The scheduler is implemented preferably in an application program in the access point controller.

Because full-duplex communication is needed in local area networks, also a full-duplex data transmission connection is needed on the radio channel. In a time division system, this can be implemented either in such a way that some of the time slots in a frame are allocated for transmission from the mobile terminal to the access point (uplink) and some are allocated for transmission from the access point to the mobile terminal (downlink), or in such a way that a separate frequency band is allocated for each communication direction. In the HIPERLAN/2 system, the introduction of the first mentioned method is proposed, wherein the access point and the terminals coupled therewith do not transmit simultaneously.

When the data transmission is being set up, the mobile terminal is listening to find out which access points have signals to be received. The mobile terminal advantageously measures the strength of the signals and selects the access point whose signal is the strongest at the moment. Thereafter the mobile terminal and the access point conduct connection set-up signalling for instance to transmit parameters such as the required data transmission rate, connection type, data transmission channel, time slots, and connection identifier to be used in the connection.

Typically also during the connection, the mobile terminal measures the strength of the signal of the access point used in the connection as well as the strength of the signals of the other possible access points within the coverage area. If it is detected that the signal strength of another access point is sufficiently greater than the signal strength of the access point used at that particular moment, it is possible to conduct a handover to this access point, which is known as such.

The HIPERLAN/2 communication system comprises an access point AP, an access point controller APC, and mobile terminals MT. Furthermore, the HIPELAN/2 system can be arranged in a data transmission connection with other communication systems, such as public switched and mobile telecommunication networks, the Internet network, *etc.* Communication between the access point and the mobile terminal is effected in a wireless manner on the radio channel. Thus, to reduce the risk of eavesdropping, encryption can be performed, whereby informa-

tion intended to be transmitted on the radio channel is first encrypted and then transmitted. For encryption, a set of encryption keys is proposed to be established in the HIPERLAN/2 communication system. The keys of this set of encryption keys are used in a predetermined order to encrypt information contained in a data frame to be transmitted each time. The length of the encryption key is *e.g.* 56 bits. This encryption key and a particular encryption algorithm are used to form encrypted information. The encryption algorithm and the set of encryption keys are stored at the access point as well as in the mobile terminals. Thus, the encryption algorithm and the encryption keys do not need to be transmitted over the radio channel, which reduces the risks of uncovering the encryption method and of misuse.

To make the uncovering of the encryption key and the encryption algorithm more difficult, the same encryption key is not used continuously, but the encryption keys is changed at certain intervals. For this reason, such a solution has been proposed for the HIPERLAN/2 system that a so-called encryption number (synchronization seed for the encryption key) is transmitted from the access point to the mobile terminal, on the basis of which the mobile terminal can form the encryption key used in the description. The encryption number (and the encryption key) is always frame-specific; that is, it is changed at intervals of two milliseconds in the HIPERLAN/2 system. However, this encryption number does not need to be transmitted to the mobile terminal for each frame separately, but the arrangement is implemented in such a way that the mobile terminal knows the encryption key sequence and can, on the basis of one encryption number received, find out also the encryption key to be used in the encryption of the next frames. However, this requires that the mobile terminal remains synchronized with the transmission of the access point. If, for any reason, the mobile terminal does not detect all the frames, or the mobile terminal is, for any other reason, no longer synchronized with the transmission of the access point, the mobile terminal does not have correct information on the encryption key. Also in a situation in which the mobile terminal has performed handover, the mobile terminal has no information about the encryption key used by this new access point at each time. For this reason, it has been proposed that the transmission of the encryption number be performed at predetermined intervals, wherein the mobile terminal will be,

again, capable of performing encryption/decryption after the mobile terminal has received the new encryption number.

The transmission interval of encryption numbers affects *e.g.* the fact how fast, for example in a handover situation, the mobile terminal is capable of transmitting encrypted information. Thus, the faster the encryption numbers are transmitted, the sooner after a handover the mobile terminal is capable of transmitting and receiving encrypted information. This short transmission interval of the encryption numbers will, however, cause the disadvantage that the communication system is loaded to a relatively great extent by these transmissions of encryption numbers.

It is an aim of the present invention to provide a method and a communication system, whereby the interval of transmitting encryption numbers can be extended and a fast recovery can still be achieved for example in a handover situation and upon failure of synchronization. The invention is based on the idea that the access point transmits the encryption number to the mobile station in connection with the handover. The method according to the present invention is characterized in what will be presented in the characterizing part of the appended claim 1. The communication system according to the present invention is characterized in what will be presented in the characterizing part of the appended claim 9.

With the present invention, significant advantages are achieved when compared with solutions of prior art. Using the method of the invention, it is possible to spread the interval of transmitting encryption numbers and still to perform synchronization with the encryption in a mobile terminal quickly in a handover situation. Because the interval of transmitting the encryption numbers can be spread, also the loading of the communication system is reduced correspondingly, as also the processing required at the access point and in the mobile terminal. Furthermore, the total power consumption of mobile terminals can be reduced, because the mobile terminal is not unnecessarily shifted from a sleep mode to a normal operation mode to receive data frames, in which an encryption number is transmitted to another mobile terminal. Fast synchronization with the encryption also means that in handover

situations, disconnections can be avoided better than in communication systems of prior art.

In the following, the present invention will be described in more detail with reference to the appended drawings, in which

Fig. 1a shows a communication system according to a preferred embodiment of the invention in a reduced block chart,

Fig. 1b shows a data frame in the HIPERLAN/2 system,

Fig. 2 shows a mobile terminal according to a preferred embodiment of the invention in a reduced block chart,

Fig. 3 shows an access point and an access point controller according to a preferred embodiment of the invention in a reduced block chart,

Fig. 4 shows, in a reduced manner, the implementation of the method according to a preferred embodiment of the invention in a data frame format,

Fig. 5 shows, in a reduced manner, encryption implemented in connection with the method according to a preferred embodiment of the invention in a reduced chart, and

Fig. 6 shows protocol stacks to be applied in a communication system according to a preferred embodiment of the invention in a reduced manner.

In the following description of a communication system 1 according to a preferred embodiment of the invention, the HIPERLAN/2 system of Fig. 1a will be used as an example, but it is obvious that the invention is not limited solely to this system. The communication system 1 consists of mobile terminals MT1—MT4, one or several access points AP1, AP2, as well as access point controllers APC1, APC2. A radio connection is set up between the access point AP1, AP2 and the mobile station MT1—MT4, for transmitting *e.g.* signals required for setting up a

connection and information during the connection, such as data packets of an Internet application. The access point controller APC1, APC2 controls the operation of the access point AP1, AP2 and the connections set up via them to mobile terminals MT1—MT4. The access point controller APC1, APC2 has a controller 19 (Fig. 3), functions of the access point being implemented in its application software, including an access point scheduler for performing various scheduling operations in a way known *per se*. In such a radio network, several access point controllers APC1, APC2 can communicate with each other as well as with other data networks, such as the Internet network, a UMTS mobile communication network (Universal Mobile Terminal System), *etc.*, wherein the mobile terminal MT1—MT4 can communicate *e.g.* with a terminal TE1 coupled to the Internet network. It is obvious that the invention can also be applied in such communication systems which have no access point controller APC1, APC2 but where the corresponding functions are implemented at the access point AP1, AP2.

Figure 2 shows, in a reduced block chart, a mobile terminal MT1 complying with a preferred embodiment of the invention. The mobile terminal MT1 preferably comprises data processing functions PC and communication means COM to set up a data transmission connection to a mobile local area network. The mobile terminal can also be formed in such a way that a data processor, such as a portable computer, is connected *e.g.* with an expansion card comprising said communication means COM. The data processing functions PC preferably comprise a processor 2, such as a microprocessor, a microcontroller or the like, a keypad 3, a display means 4, memory means 5, and connection means 6. In addition, the data processing functions PC can comprise audio means 7, such as a speaker 7a, a microphone 7b, and a codec 7c, wherein the user can use the mobile terminal MT1 also *e.g.* for the transmission of speech. Information intended to be transmitted from the mobile terminal MT1 to the local area network is preferably transmitted by the connection means 6 to the communication means COM. In a corresponding manner, information received from the local area network 1 into the mobile terminal MT1 is transmitted to the data processing functions PC via said connection means 6.

The communication means COM comprise *e.g.* an antenna 30, a high-frequency part 8, an encoder 20, a decoder 21, an encryption block 9, a decryption block 10, a control means 11, as well as a reference oscillator 12. The high-frequency part 8 preferably comprises *e.g.* filters, a modulator and a demodulator (not shown). Furthermore, the communication means COM have a memory 13 for example for forming the transmission and receiving buffers required in the data transmission as well as for storing the encryption key table and the encryption sequence. The encoder 20 is used for encoding information contained in data frames. The encoded information is transmitted to the high-frequency part 8 to be modulated and to be transmitted as a radio-frequency signal in the communication channel CH (Fig. 1a). In a corresponding manner, in the decoder, the encoded information received from the communication channel and demodulated in the demodulator is restored preferably into data frame format. The reference oscillator 12 is used to perform the necessary scheduling to synchronize the transmission and reception with the transmission and reception of the access point. The reference oscillator 12 can also be used for generating timing signals for the control means 11, wherein in practical applications, frequency conversion means (not shown) are used to convert the frequency of the reference oscillator 12 into frequencies needed in the radio part and a frequency suitable for controlling the operation of the control means 11.

The access point AP1 (Fig. 3) comprises, in a corresponding manner, first communication means 15, 23—26 for setting up a data transmission connection to mobile terminals MT1—MT4. The local area network according to the invention can also be implemented as a local area network with no connection to external data networks. Thus, one access point AP1 may be sufficient, with which the mobile terminals MT1—MT4 of the local area network communicate. In the mobile local area network, a data transmission connection 16 is preferably arranged from one or several access points AP1, AP2 to a data processor S which is generally called a server computer or, shorter, a server. Such a server comprises, in a way known *per se*, company data files, application software, *etc.* in a centralized manner. The users can thus start up applications installed on the server S via the mobile terminal MT1. The server S or the access point AP1 may also comprise second

communication means 17 to set up a data transmission connection to another data network, such as the Internet network or a UMTS mobile communication network.

The communication means of the access point AP1, AP2 comprise one or several oscillators 22 to generate the frequencies needed in the operation, an encryption block 23, a decryption block 25, an encoder 24, a decoder 26, as well as a high-frequency part 15, which are known *per se*.

Each access point AP1, AP2 and mobile terminal MT1—MT4 is allocated an identification, wherein the access point AP1, AP2 is aware of the mobile stations MT1—MT2 coupled to the access point AP1, AP2. In a corresponding manner, on the basis of the identifications, the mobile terminals MT1—MT4 separate the frames transmitted by different access points AP1, AP2 from each other. These identifications can also be used in a situation in which the connection of the mobile terminal MT1—MT4 is handed over from one access point AP1 to another access point AP2, *e.g.* as a result of impaired quality of the connection.

For communication, the mobile terminal MT1 must be coupled in a data transmission connection with the local area network 1. This can be performed preferably in such a way that a network controller, or a corresponding application program is started up in the mobile terminal MT1, containing the program codes for logging in the local area network 1 as well as for transmitting data between the mobile terminal MT1 and the local area network 1. In connection with starting up the network controller, the necessary operations are performed *e.g.* to set up the functional parameters of the communication means COM of the mobile terminal. Thus, the receiver of the communication means COM starts to receive signals at a channel frequency of the local area network. If no signal is detected within a certain time, the channel to be listened to is changed. At the stage when a signal is detected on any channel frequency, the signal received by the receiver of the communication means COM is demodulated and transmitted to be decoded, wherein it is possible to determine the information transmitted in the radio signal, which is known as such. This decoded signal, which is preferably stored in the receiving buffer in the memory 13 of the communication means, is

searched for the identifier of the BCCH control field of the data frame. The identifier of this BCCH control field is located at a particular point in the data frame, and therefore, after the identifier is found, the location of the BCCH control field in the receiving buffer is known. The BCCH control field contains for instance the identifier (AP ID) of the access point that has transmitted the frame FR1, the identifier of the local area network (NET ID), the data frame number, the encryption number, the initializing vector, if necessary, as well as information on the length of the FCCH control field, the way of modulation, and encoding.

The mobile terminal MT1 is synchronized with the transmission of this access point AP1. The mobile terminal MT1 requests for connection set-up by transmitting an RACH message to the access point AP1 at a moment of time allocated for the same. For example, in the frame structure according to Fig. 1b, the RACH message can be transmitted after the transmission and reception time slots, before the next BCCH control field. In the message, the mobile terminal MT1 transmits information *e.g.* on the quality of service requested for the connection and on the connection type, such as a multimedia connection, data connection, speech connection. The connection type and the quality of service influence *e.g.* the number of time slots TS1—TSn to be allocated for the connection.

The access point controller APC1 examines the message and finds out, *e.g.* from a resource allocation table or the like, how much resources are available at the time for the access point AP1. If there are sufficient resources to set up a connection corresponding to the requested quality of service, the access point controller APC1 allocates the required resources for the connection. In the memory means 14 of the access point controller APC1, transmission and receiving strings (buffers) are formed for the connection, which are used for temporary storage of received packets and for temporary storage of packets waiting to be transmitted. Furthermore, each connection is allocated a connection identifier, wherein the transmission of data to the correct destination is secured. Also, priority can be selected for the connection, wherein resources available at the time, such as transmission and receiving time slots, are allocated in the order of priority. Depending on *e.g.* the need for resources, it is possible to allocate a different number of time

slots TS1—TSn from the data field of the data frame FR for different connections. Also, the number of time slots allocated for transmission and for reception can be different even in the same connection, as already mentioned above in this description. The number of time slots TS1—TSn allocated for connections may also vary according to the frame, wherein in each frame FR, the number of time slots TS1—TSn allocated for the connection may vary from zero to a maximum. The location of the transmission and receiving time slots contained in the data frame is preferably transmitted in the FCCH control field.

After a connection to the local area network 1 has been set up, it is possible to start data transmission between a server S and a mobile terminal MT1 preferably with a protocol, such as the IP (Internet Protocol). Figure 6 shows this data transmission by means of protocol stacks. Of the protocol stacks, the application layer AL, the convergence layer + network layer CL+NL, the data link layer DL, and the physical layer PHY are presented. On the radio channel, *i.e.* between the access point AP1 and the mobile terminal MT1, the data link layer of the protocol stack comprises, in this preferred embodiment, the MAC layer (Media Access Control) as the lowermost layer, which takes care of using the radio channel in communication between the mobile terminal MT1 and the access point AP1, such as encryption and channel allocation in the transmission and reception of packets. This description deals primarily with data frames FR of the MAC layer. It is obvious that encryption operations can also be performed in connection with the other protocol layers, but this is not significant *per se* in view of this invention, wherein they are not discussed in more detail in this context.

A scheduler 18 formed in the access point controller APC1, APC2 performs *e.g.* scheduling of data frames FR of the access point AP1, AP2 and allocation of transmission and receiving time slots for packets of active connections waiting to be transmitted. The scheduler switches the receiver of the access point to receive a radio signal for the time allocated for the RACH field of the frame. Thus, mobile terminals MT1—MT4 can transmit, in addition to the above-presented connection set-up request, various measurement data to the access point.

In the following, the operation of the method according to a preferred embodiment of the invention will be described. At the stage when the mobile terminal MT1 has been connected to the first access point AP1 and has received an encryption number KI, the mobile terminal MT1 has set an encryption sequence counter SC (Fig. 2) to a value corresponding to the encryption number. If the encryption number is an index referring to an encryption key table ST, one advantageous example being shown in Fig. 5, the value of the encryption key table ST can be set directly to this encryption number. After this, the mobile terminal MT1 monitors the transmission of the access point AP1 and always in connection with frame change changes the value of the encryption sequence counter in such a way that it preferably indicates the next encryption key in the encryption key table ST. The frame change can be detected in that the access point AP1 transmits the (next) BCCH control field. In connection with receiving this BCCH control field, the mobile terminal MT1 can, if necessary, also perform synchronization of the local clock to keep it synchronized with the access point AP1. After the last encryption key in the encryption table ST, the encryption sequence counter SC is preferably set to indicate the start of the encryption table ST.

In the BCCH field of certain MAC frames, the access point AP1 transmits information to all mobile terminals connected with the access point AP1 in question (broadcast frame) or to some of them (subbroadcast frame). Thus, each of these mobile terminals receives at least the information transmitted in the BCCH field and uses it to find out when information is transmitted to the mobile terminal in question and when it can transmit information. After this, the mobile terminal can possibly shift to a sleep mode to save power, wherein the sleep mode is set to terminate either before the transmission of the next general BCCH control field intended for several mobile terminals, or before the transmission or receiving time slot allocated for the mobile terminal MT1 in question. In the sleep mode, the radio part of the mobile terminal MT1 is set in a power saving mode or turned off. The encryption sequence counter SC can, however, be updated, because the mobile terminal MT1 is aware of the number of MAC frames during which it is in the sleep mode.

Encryption in a communication system according to a preferred embodiment of the invention is presented in the appended Fig. 5 in a reduced chart. An encryption number KI and, if necessary, also an initialization vector IV are transmitted at least once to the mobile terminal MT1. The initialization vector has a certain initial value set for a random sequence generator RS. The initial value for the random sequence generator of the mobile terminal is set in a corresponding manner in the mobile terminal MT1. At the stage when the access point AP1 has information to be transmitted to the mobile terminal, an encryption sequence is formed in the random sequence generator RS on the basis of the encryption key in use at the moment. This encryption sequence is transferred to a combination block XOR in which an Exclusive Or (XOR) operation is preferably performed between the encryption sequence and the information to be transmitted, to produce information encrypted bit by bit. From the combination block XOR, the encrypted information is transferred further to be transmitted in preferably one or several data fields D.

The communication means COM of the mobile terminal MT1 are used to decrypt information received from the communication channel and demodulated in the demodulator, preferably in the following way. In the mobile terminal MT1, the encryption sequence is calculated on the basis of the encryption key, the random sequence generator and the initializing vector in the same way as in the access point AP1. The encrypted information and the encryption sequence are transferred to a separation block XOR', whose output comprises the transmitted information in unencrypted form.

It is obvious that in connection with the present invention, also other methods for encrypting information with an encryption key can be used than that presented above.

In a situation in which the mobile terminal MT1 hands the connection over to a second access point AP2 or the first access point AP1 performs a forced handover, the mobile terminal MT1 performs the normal handover signalling with this second access point AP2. This is described as a frame indicated with the reference HO in the appended Fig. 4. At this stage, the mobile terminal MT1 can, however, no longer

use the encryption number in its memory, because the mobile terminal MT1 does not known which encryption number is used at this second access point AP2 at the moment. The second access point AP2 transmits the encryption number at intervals, but in addition to that, in the method according to the present invention, the access point AP2 will send the encryption key after the handover, because the time until the next transmission of the encryption number can be so long that the connection could even be cut off.

The transmission of the encryption key can be preferably implemented in the following way (Fig. 4). After receiving information about a need to transmit the encryption number, the second access point AP2 selects the next suitable moment for the transmission of the encryption key. The access point AP2 preferably selects such a BCCH control field which is not used as a general BCCH control field mentioned above in this description, indicated as an example with the reference BC in Fig. 4. By this arrangement, receiving operations are not caused unnecessarily and power consumption is not unnecessarily increased in other mobile terminals. The access point AP2 transmits the encryption number at least once, but to secure that the mobile terminal MT1 receives the encryption number correctly, the access point can also retransmit it several times, for example three times in succession. This retransmission may be necessary *e.g.* in such situations in which the mobile terminal MT1 is at the edge of a cell or in another location where the signal strength is decayed. Figure 4 shows, indicated with the reference YS, the transmission of one or more encryption numbers to be transmitted after the handover and, indicated with the reference NS respectively, the normal transmission of the encryption number to be performed at intervals.

The handover can be reported to the access point AP1, AP2 in several different ways. For example, a mobile terminal MT1 communicating with one access point AP1 can transmit a handover request to another access point AP2. In this connection, the mobile terminal MT1 can inform about the handover to the access point AP1 with which it communicates at the moment and from which the connection is handed over to the second access point AP2. Thus, if a data transmission connection is arranged between the access points AP1, AP2, this first

access point AP1 can inform the second access point AP2 that there is a need to transmit the encryption numbers more often. Another alternative is that the access point AP1 with which the mobile terminal MT1 communicates at the moment, forces the mobile terminal MT1 to execute the handover. Also in this situation, this first access point AP1 can inform the second access point AP2 that there is a need to transmit the encryption numbers more often.

At the access point AP1, AP2, the operations of the method according to the invention can be preferably implemented in the application software of the controller 19 of the access point controller.

The invention can also be applied in other systems than the HIPERLAN/2 system used in this example. For example in the mobile communication system according to the GSM system (not shown), a base transceiver station corresponds to the access point AP1, AP2, and a base station controller corresponds to the access point controller APC1, APC2, being in radio communication with the mobile terminals via the base stations.

In a corresponding manner, in the WCDMA system (not shown), a node-B corresponds to the access point AP1, AP2 and a radio network controller corresponds to the access point controller APC1, APC2.

Also other than time division multiple access (TDMA) systems are feasible, *e.g.* a code division multiple access (CDMA) system, or a frequency division multiple access (FDMA) system, or a combination of these different systems. Thus, in the code division multiple access system, the feature corresponding to the time slots (transmission sequence) is a code slot, and in the frequency division multiple access system it is a frequency slot.

It is obvious that the present invention is not limited solely to the above-presented embodiments, but it can be modified within the scope of the appended claims.

Claims:

1. A method for transmitting an encryption number in a communication system (1) comprising mobile terminals (MT1—MT4) and at least a first access-point (AP1) and a second access point (AP2), the method comprising the steps of:

— defining a set of encryption keys,

— selecting at each said access point (AP1, AP2) from said set of encryption keys one to be used at a time for encrypting information to be transmitted between said access point (AP1, AP2) and mobile terminal (MT1—MT4),

— transmitting from the access point (AP1, AP2), at intervals, data about the encryption key selected at the time,

— setting up a data transmission connection between a mobile terminal (MT1—MT4) and the first access point (AP1) for the transmission of information, and

— performing a handover, whereby a data transmission connection is set up between the second access point (AP2) and the mobile terminal (MT1—MT4),

characterized in that in the method, in connection with the handover, information is transmitted to the mobile terminal (MT1—MT4) about the encryption key selected at the second access point (AP2).

2. The method according to claim 1, **characterized** in that each encryption key in said set of encryption keys is allocated an encryption number (KI), wherein said encryption number (KI) is used as said data about the encryption key selected.

3. The method according to claim 1 or 2, in which information is transmitted in data frames (FR), **characterized** in that the encryption key is changed in connection with each data frame (FR).

4. The method according to claim 3, in which some of the data frames are used as common data frames for transmitting information from the second access point (AP2) to more than one mobile terminal (MT1—MT4), **characterized** in that said data about the encryption key is transmitted in another data frame than said common data frame.

5. The method according to any of the claims 1 to 4, **characterized** in that said set of encryption keys is stored in said access points (AP1, AP2) and in the mobile terminal (MT1—MT4).

6. The method according to any of the claims 1 to 5, **characterized** in that the mobile terminal (MT1—MT4) informs said second access point (AP2) about a need for handover, wherein said second access point (AP2) transmits information about the encryption key selected at the second access point (AP2) at the moment to the mobile terminal (MT1—MT4).

7. The method according to any of the claims 1 to 5, **characterized** in that the mobile terminal (MT1—MT4) informs said first access point (AP1) about a need for handover, that said first access point (AP1) transmits information about the handover to said second access point (AP2), wherein said second access point (AP2) transmits information about the encryption key selected at the second access point (AP2) at the time to the mobile terminal (MT1—MT4).

8. The method according to any of the claims 1 to 5, **characterized** in that the first access point (AP1) executes a forced handover, in which the mobile terminal (MT1—MT4) communicating with said first access point is transferred to communicate with said second access point (AP2), that said first access point (AP1) transmits information about the handover to said second access point (AP2), wherein said second access point (AP2) transmits information about the encryption key selected at the second access point (AP2) at the time to the mobile terminal (MT1—MT4).

9. A mobile communication system (1) comprising mobile terminals (MT1—MT4), at least a first access point (AP1) and a second access point (AP2); a set of encryption keys being defined in the communication system (1); the access point (AP1, AP2) comprising means for selected from said set of encryption keys one at a time to be used for encryption of information to be transmitted between said access point (AP1, AP2) and mobile terminal (MT1—MT4), and means for transmitting information about the encryption key selected at the time at intervals from the access point (AP1, AP2); the communication system (1)

also comprising means for setting up a data transmission connection between the mobile terminal (MT1—MT4) and the first access point (AP1) for the transmission of information, and means for executing a handover and setting up a data transmission connection between the second access point (AP2) and the mobile terminal (MT1—MT4), **characterized** in that the mobile communication system (1) also comprises means for transmitting information about the encryption key selected at the second access point (AP2) to the mobile terminal (MT1—MT4) in connection with the handover.

10. The mobile communication system (1) according to claim 9, **characterized** in that it also comprises means for defining an encryption number for each encryption key in said set of encryption keys (ST), wherein said encryption number (KI) is arranged to be used as said information about the encryption key selected.

11. The mobile communication system (1) according to claim 9 or 10, which comprises means for transmitting information in data frames (FR), **characterized** in that the encryption key is arranged to be changed in connection with each data frame (FR).

12. The mobile communication system (1) according to claim 11, in which some of the data frames are arranged to be used as common data frames for transmitting information from one access point (AP2) to more than one mobile terminal (MT1—MT4), **characterized** in that said data about the encryption key is arranged to be transmitted in another data frame than said common data frame.

13. The mobile communication system (1) according to any of the claims 9 to 12, **characterized** in that said set of encryption keys is stored at said access points (AP1, AP2) and mobile terminal (MT1—MT4).

14. The method according to any of the claims 9 to 13, **characterized** in that the mobile terminal (MT1—MT4) comprises means (8, 11, 30) for informing said second access point (AP2) about the need for a handover, wherein data is arranged to be transmitted from said second

access point (AP2) to the mobile terminal (MT1—MT4) about the encryption key selected at the second access point (AP2) at the time.

15. The method according to any of the claims 9 to 13, **characterized** in that the mobile terminal (MT1—MT4) comprises means (8, 11, 30) for informing said first access point (AP1) about the need for handover,

16. The method according to any of the claims 9 to 13, **characterized** in that the first access point (AP1) comprises means for performing a forced handover, wherein the mobile terminal (MT1—MT4) communicating with said first access point is arranged to be handed over to communicate with said second access point (AP2), and means for transmitting information about the handover to said second access point (AP2), wherein information about the encryption key selected at the second access point (AP2) at the time is arranged to be transmitted from said second access point (AP2) to the mobile terminal (MT1—MT4).

Abstract

The invention relates to a method for transmitting an encryption number in a communication system (1) comprising mobile terminals (MT1—MT4) and at least a first access point (AP1) and a second access point (AP2). The method comprises the steps of defining a set of encryption keys, selecting at each said access point (AP1, AP2) from said set of encryption keys one to be used at a time for encrypting information to be transmitted between said access point (AP1, AP2) and mobile terminal (MT1—MT4), transmitting from the access point (AP1, AP2), at intervals, data about the encryption key selected at the time, setting up a data transmission connection between a mobile terminal (MT1—MT4) and the first access point (AP1) for the transmission of information, and performing a handover, whereby a data transmission connection is set up between the second access point (AP2) and the mobile terminal (MT1—MT4). In the method, a handover is performed, wherein a data transmission connection is set up between the second access point (AP2) and the mobile terminal (MT1—MT4). In the method, in connection with the handover, information is also transmitted to the mobile terminal (MT1—MT4) about the encryption key selected at the second access point (AP2).

Fig. 4

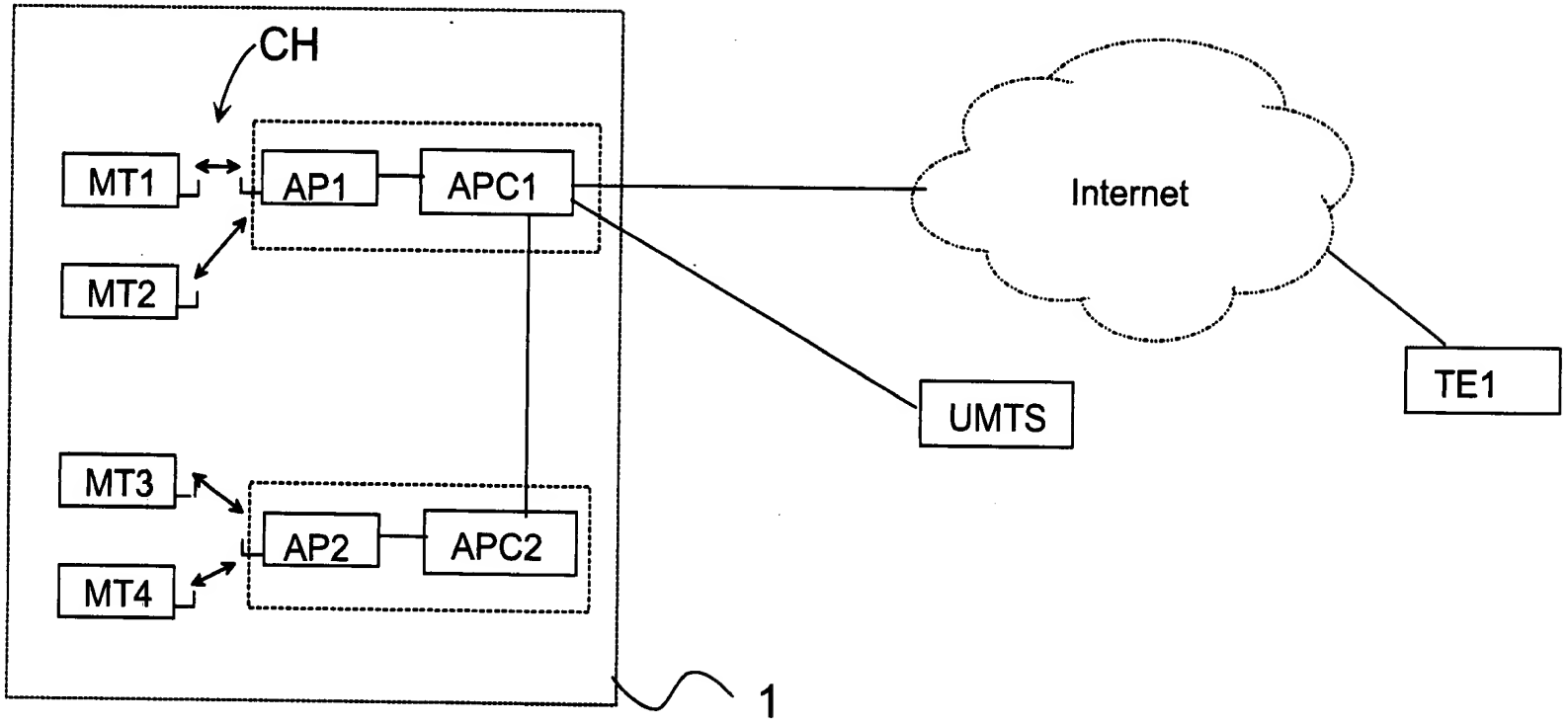

Fig. 1a

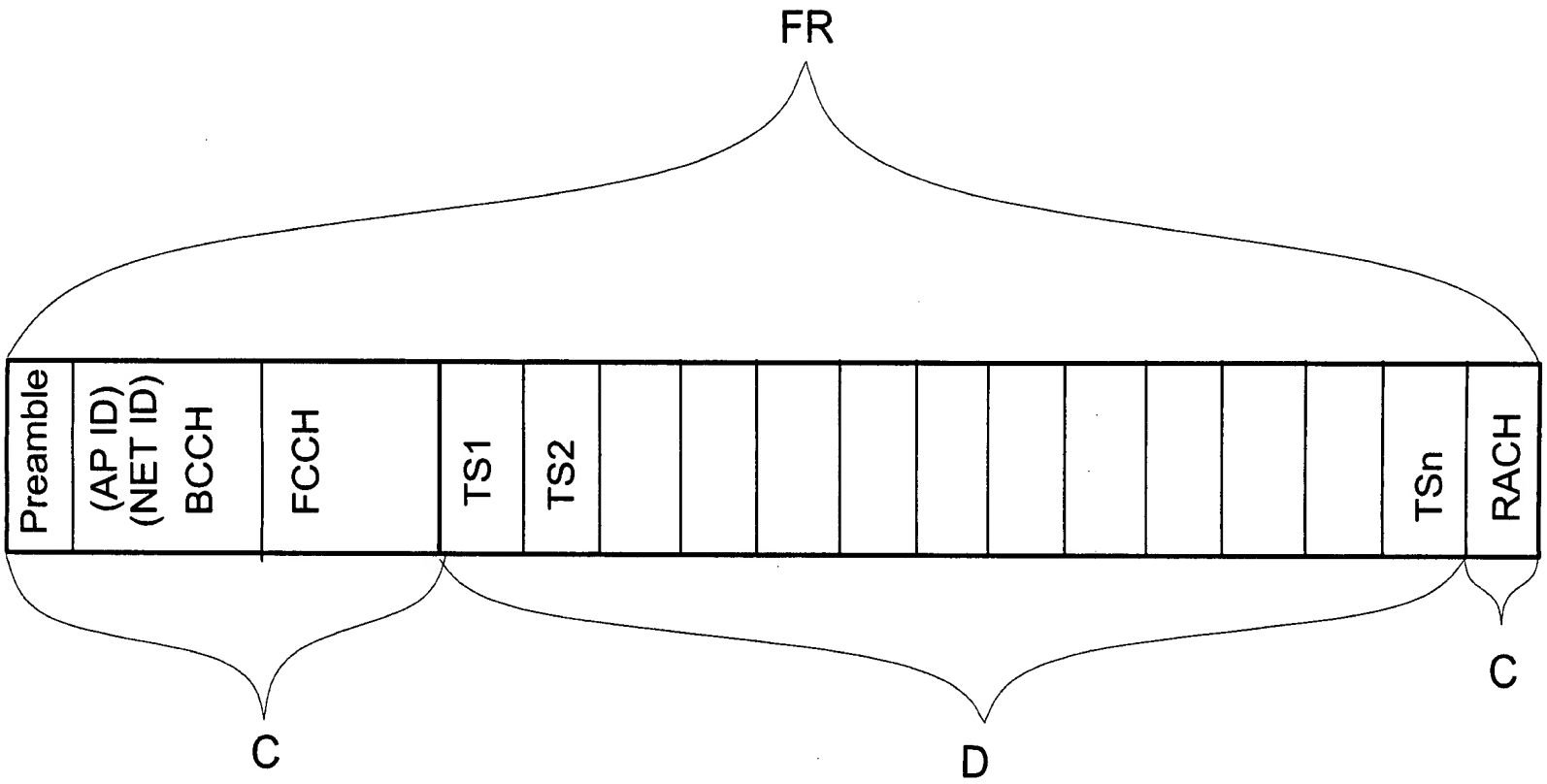

Fig. 1b

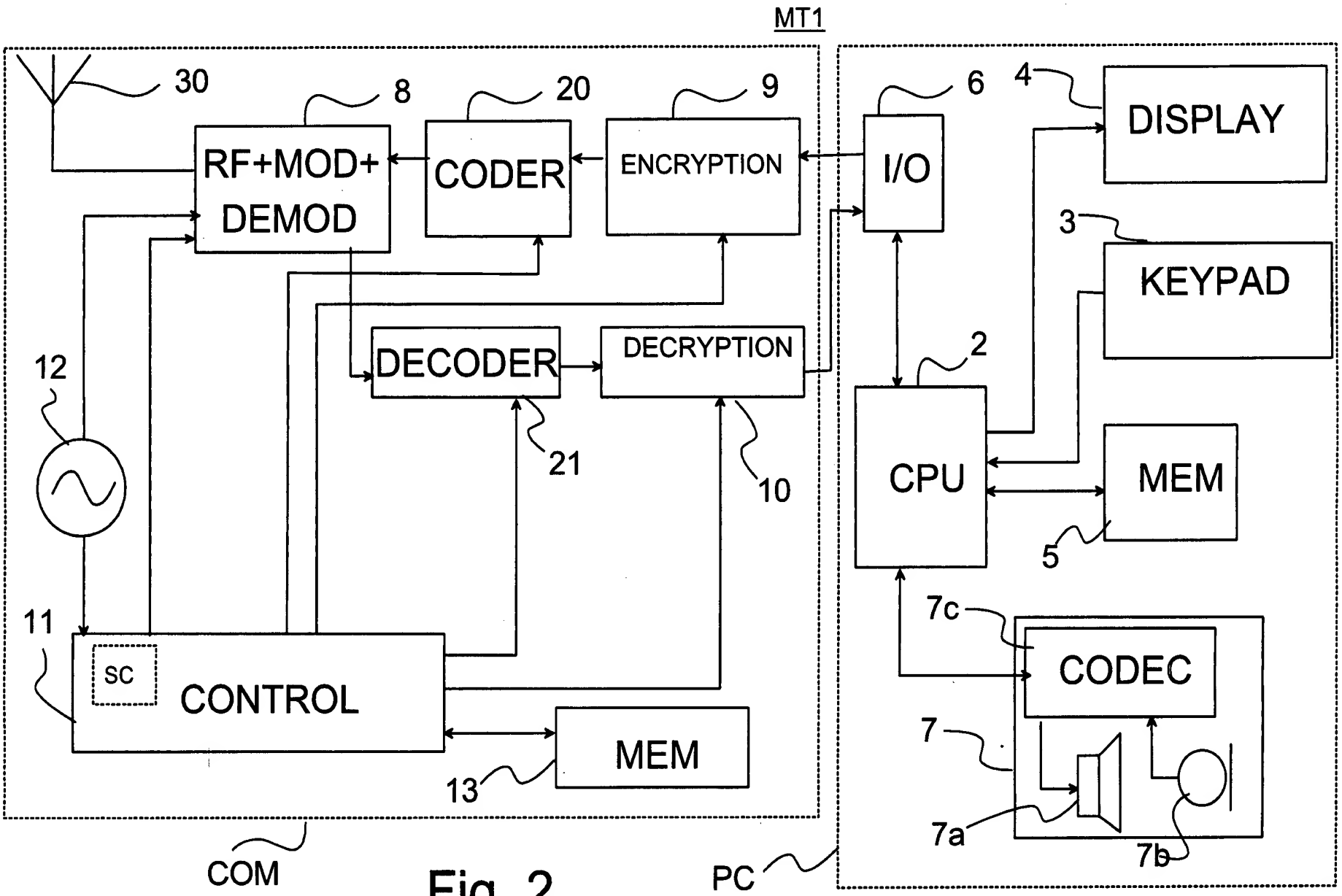
MT1
30
8
20
9
6
4
DISPLAY
RF+MOD+
DEMOD
CODER
ENCRYPTION
I/O
3
KEYPAD
12
DECODER
DECRYPTION
2
21
10
CPU
MEM
5
11
7c
SC
CONTROL
CODEC
7
MEM
13
7a
7b
COM
PC

Fig. 2

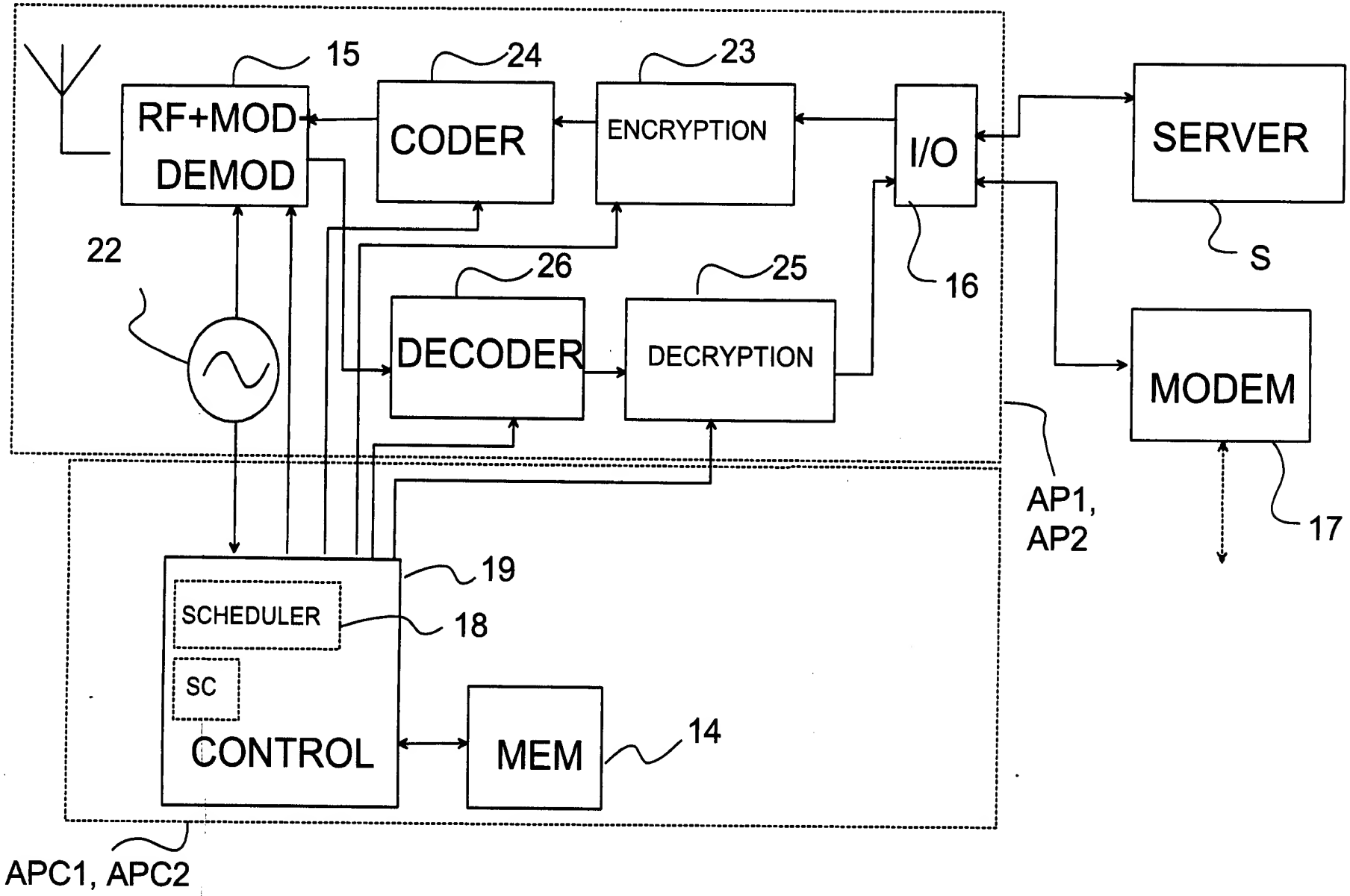
15
24
23
RF+MOD
DEMOD
CODER
ENCRYPTION
I/O
SERVER
22
26
25
16
S
DECODER
DECRYPTION
MODEM
AP1,
AP2
17
19
SCHEDULER
18
SC
CONTROL
MEM
14
APC1, APC2

Fig. 3

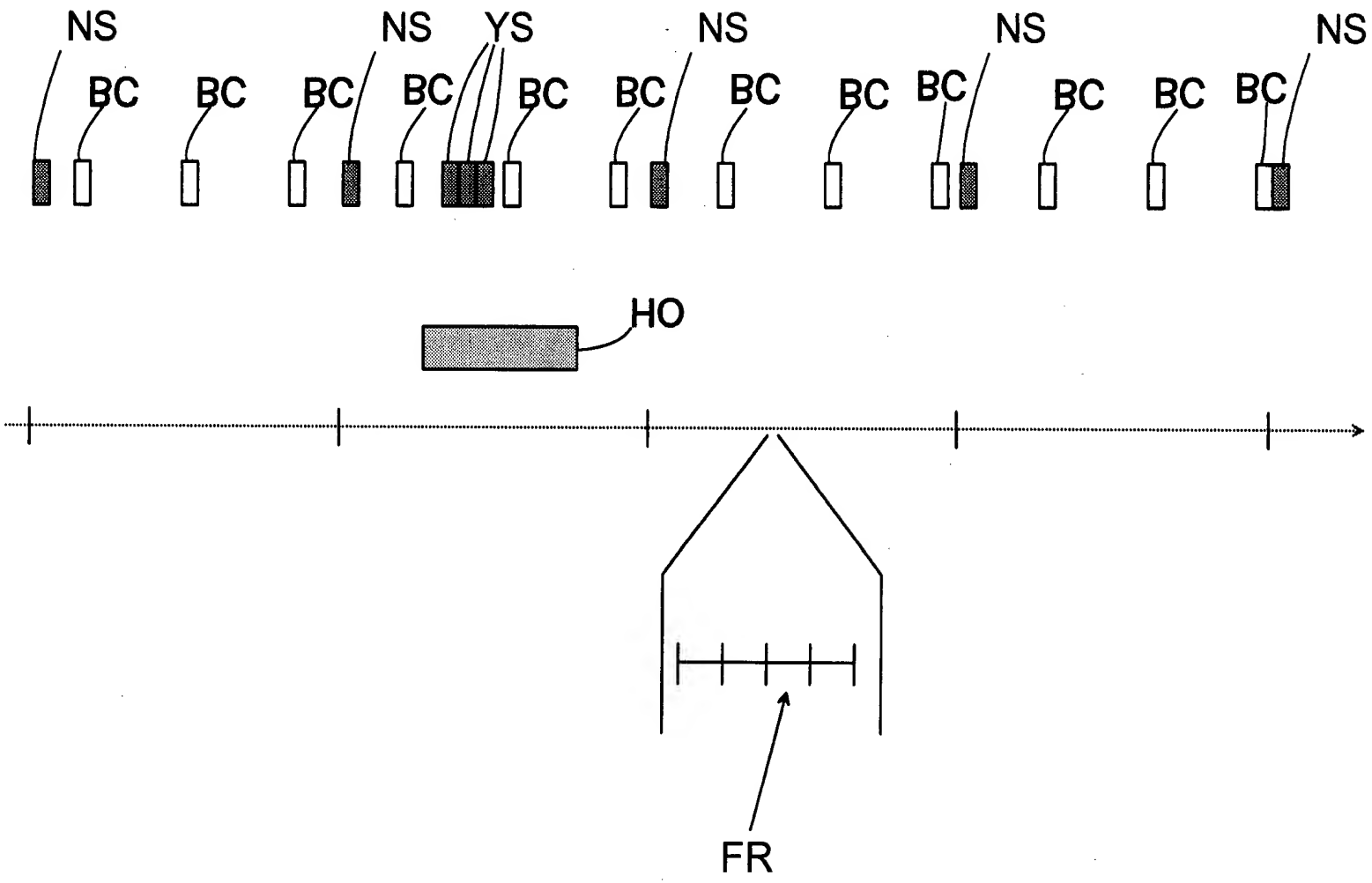

Fig. 4

KI1	Key 1
KI2	Key 2
KI3	Key 3
KI4	Key 4
KI5	Key 5
KIm-1	Key M-1
KIm	Key M

ST

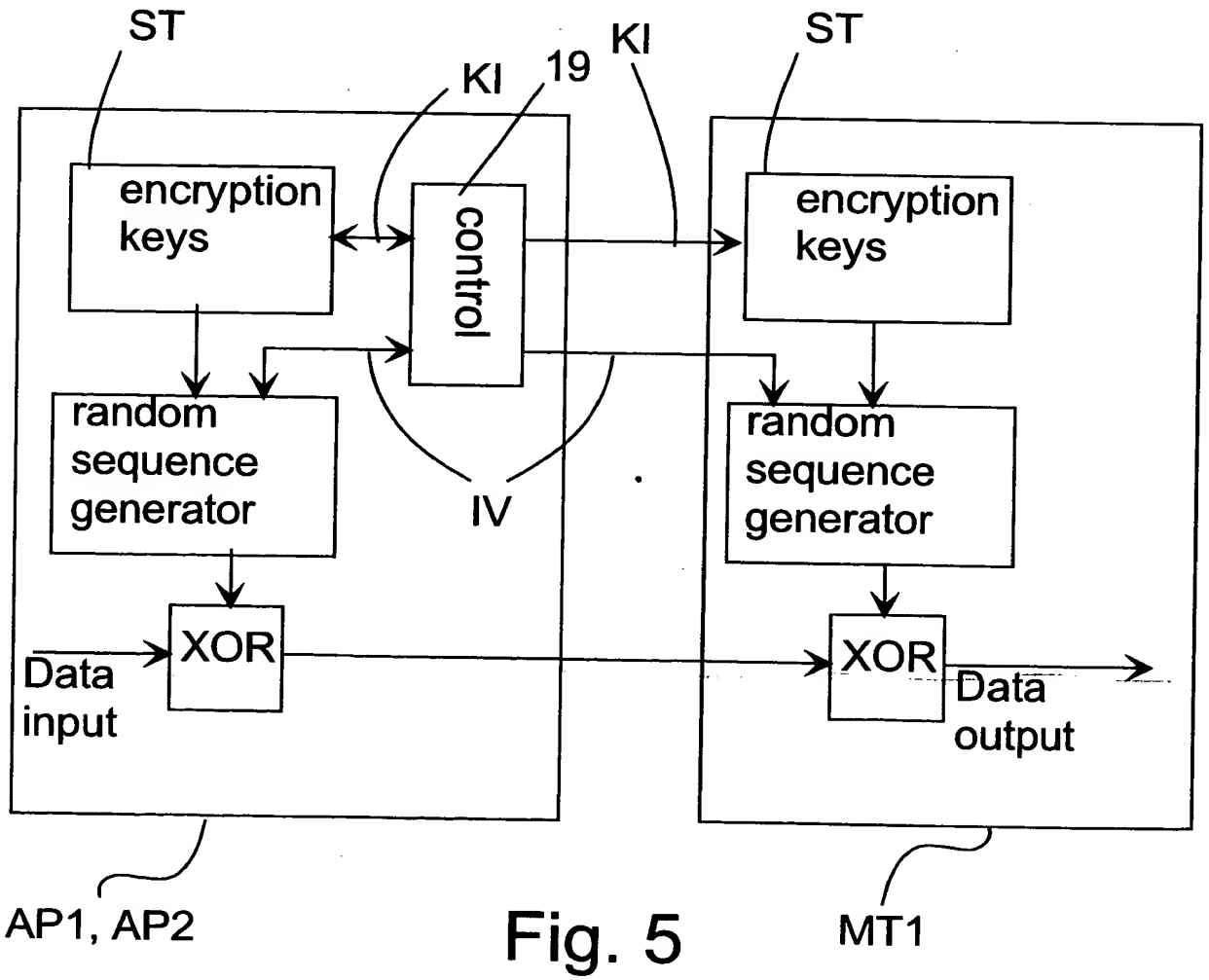

Fig. 5

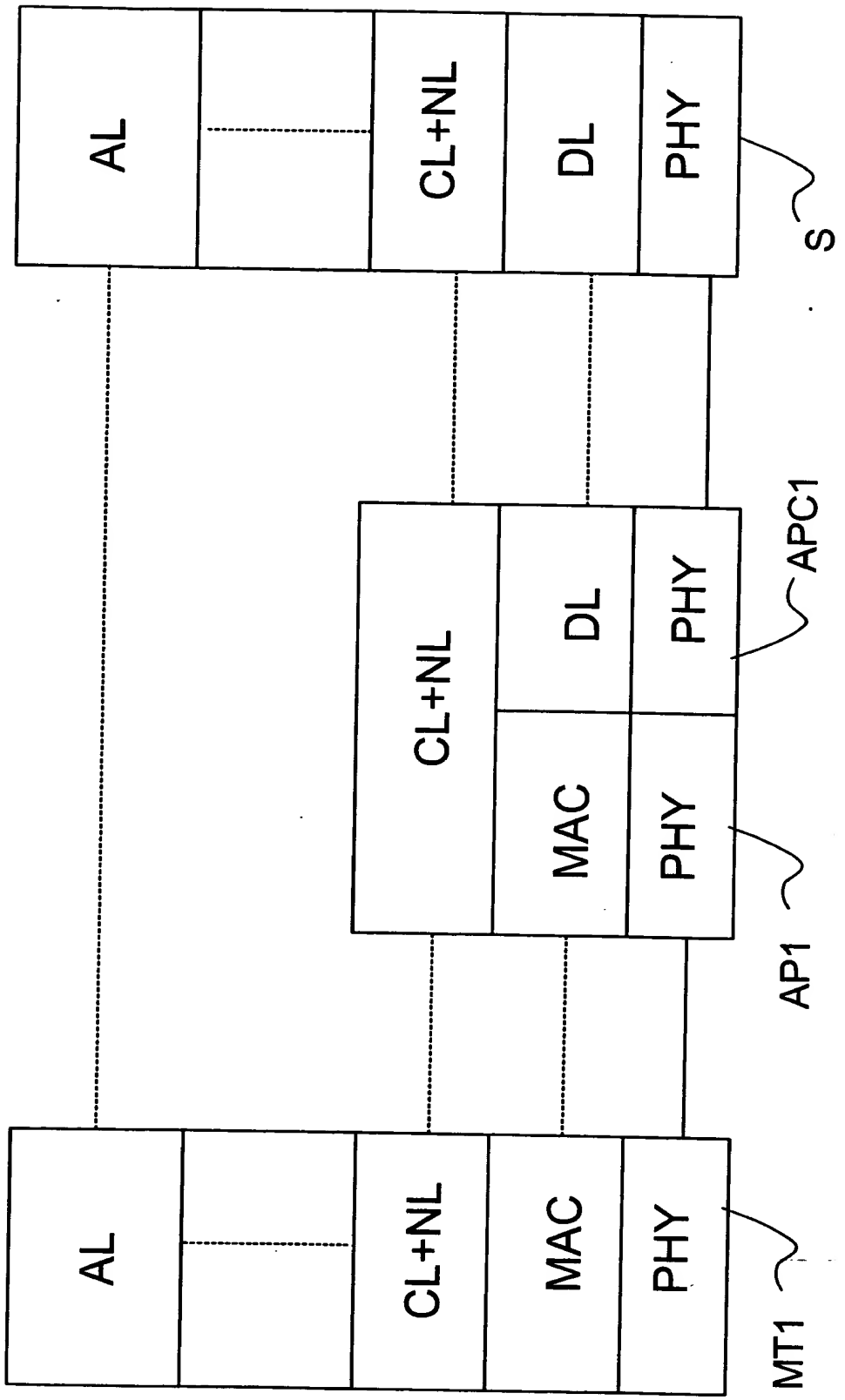

Fig. 6